Atty. Dkt. No. 062800-0103

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Yasutaka SATO

Title: MODEM DEVICE, DATA COMMUNICATIONS SYSTEM, METHOD OF AND DEVICE FOR PROTECTING DATA AND COMPUTER PRODUCT

Appl. No.: Unassigned

Filing Date: August 9, 2001

Examiner: Unassigned

Art Unit: Unassigned

CLAIM FOR CONVENTION PRIORITY

Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

- Patent Application No. 2000-244537 filed 08/11/2000.

Respectfully submitted,

Date August 9, 2001 By 34371
Glenn Law

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5332
Facsimile: (202) 672-5399

for Kenneth E. Krosin
Attorney for Applicant
Registration No. 25,735

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　８月１１日

出願番号
Application Number: 特願２０００－２４４５３７

出願人
Applicant(s): 株式会社トリニティーコミュニケーション

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　７月２７日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０６７４７８

【書類名】　特許願
【整理番号】　TC00-003
【提出日】　平成12年 8月11日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/00
【発明者】
　【住所又は居所】　徳島市川内町平石住吉２０９番地５　株式会社トリニティーコミュニケーション内
　【氏名】　佐藤　泰崇
【特許出願人】
　【識別番号】　300023383
　【氏名又は名称】　株式会社トリニティーコミュニケーション
【代理人】
　【識別番号】　100104190
　【弁理士】
　【氏名又は名称】　酒井　昭徳
【手数料の表示】
　【予納台帳番号】　041759
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0003907
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ防護処理装置、モデム装置、データ通信システム、データ防護処理方法、その方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

【特許請求の範囲】

【請求項１】　連続するデジタルデータを順次読み込み、読み込まれたデジタルデータが所定の連続パターンの数値であるか否かを判定する判定処理手段と、

前記判定処理手段によって判定された結果、前記所定の連続パターンの数値であると判定されたデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算または減算する演算処理手段と、

を備えたことを特徴とするデータ防護処理装置。

【請求項２】　シリアル入力されたバイナリデータをバイトデータに変換して一時的に保持する保持手段と、

前記保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する判定処理手段と、

前記判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算または減算する演算処理手段と、

前記演算処理手段によって演算されたバイトデータをバイナリデータに変換してシリアル出力する出力手段と、

を備えたことを特徴とするデータ防護処理装置。

【請求項３】　シリアル入力されたバイナリデータをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する保持手段と、

前記保持手段から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出するデータ抽出処理手段と、

前記データ抽出処理手段から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判

定する判定処理手段と、

前記判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算または減算する演算処理手段と、

前記演算処理手段によって演算されたバイトデータをもちいて前記所定のデータフレームを再構成するデータフレーム再構成処理手段と、

前記データフレーム再構成処理手段によって再構成されたデータフレームをバイナリデータに変換してシリアル出力する出力手段と、

を備えたことを特徴とするデータ防護処理装置。

【請求項４】　前記演算処理手段は、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする請求項１～３のいずれか一つに記載のデータ防護処理装置。

【請求項５】　連続するデジタルデータである送信データ／受信データを順次読み込み、読み込まれた送信データ／受信データが所定の数値のデジタルデータを含んでいるか否かを判定する第１の判定処理手段と、

前記第１の判定処理手段によって、前記送信データ／受信データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算／減算する第１の演算処理手段と、

連続するデジタルデータである受信データ／送信データを順次読み込み、読み込まれた受信データ／送信データが前記所定の数値のデジタルデータを含んでいるか否かを判定する第２の判定処理手段と、

前記第２の判定処理手段によって、前記受信データ／送信データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する前記所定数のデジタルデータの全部または一部に対して、前記所定の演算値を減算／加算する第２の演算処理手段と、

を備えたことを特徴とするデータ防護処理装置。

【請求項６】　シリアル入力されたバイナリデータである送信データ／受信

データをバイトデータに変換して一時的に保持する第１の保持手段と、

前記第１の保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第１の判定処理手段と、

前記第１の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第１の演算処理手段と、

前記第１の演算処理手段によって加算／除算されたバイトデータをバイナリデータに変換して送信データ／受信データとしてシリアル出力する第１の出力手段と、

シリアル入力されたバイナリデータである受信データ／送信データをバイトデータに変換して一時的に保持する第２の保持手段と、

前記第２の保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第２の判定処理手段と、

前記第２の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第２の演算処理手段と、

前記第２の演算処理手段において減算／加算されたバイトデータをバイナリデータに変換して受信データ／送信データとしてシリアル出力する第２の出力手段と、

を備えたことを特徴とするデータ防護処理装置。

【請求項７】　シリアル入力されたバイナリデータである送信データ／受信データをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する第１の保持手段と、

前記第１の保持手段から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出する第１のデータ抽出処理手段と、

前記第１のデータ抽出処理手段から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第１の判定処理手段と、

前記第１の判定処理手段によって判定された結果、前記所定のバイトコードで

あると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第１の演算処理手段と、

前記第１の演算処理手段によって加算されたバイトデータをもちいて前記所定のデータフレームを再構成する第１のデータフレーム再構成処理手段と、

前記第１のデータフレーム再構成処理手段によって再構成されたデータフレームをバイナリデータに変換して送信データ／受信データとしてシリアル出力する第１の出力手段と、

シリアル入力されたバイナリデータである受信データ／送信データをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する第２の保持手段と、

前記第２の保持手段から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出する第２のデータ抽出処理手段と、

前記第２のデータ抽出処理手段から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第２の判定処理手段と、

前記第２の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する前記所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第２の演算処理手段と、

前記第２の演算処理手段において減算／加算されたバイトデータをもちいてデータフレームを再構成する第２のデータフレーム再構成処理手段と、

前記第２のデータフレーム再構成処理手段によって再構成されたデータフレームをバイナリデータに変換して受信データ／送信データとしてシリアル出力する第２の出力手段と、

を備えたことを特徴とするデータ防護処理装置。

【請求項８】　前記第１および第２の演算処理手段は、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする請求項５～７のいずれか一つに記載のデータ防護処理装置。

【請求項９】　さらに、前記所定の数値または所定のバイトコードに関する情報と、前記所定数に関する情報と、前記所定の演算値に関する情報と、を記憶する記憶手段と、

前記記憶手段によって記憶された前記所定の数値または所定のバイトコードに関する情報、前記所定数に関する情報、前記所定の演算値に関する情報のうちの少なくとも一つを変更する情報変更手段と、

を備えたことを特徴とする請求項１～８のいずれか一つに記載のデータ防護処理装置。

【請求項１０】　送信するデジタルデータに対して、標準化されたデータ圧縮規格に基づいてデータ圧縮処理を施すデータ圧縮手段と、

前記データ圧縮手段によってデータ圧縮処理を施されたデジタルデータをバイトデータに変換し、変換されたバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第１の判定処理手段と、

前記第１の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して所定の演算値を加算／減算する第１の演算処理手段と、

前記第１の演算処理手段において加算／減算されたバイトデータを出力する第１の出力手段と、

受信したデジタルデータをバイトデータに変換し、変換されたバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第２の判定処理手段と、

前記第２の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して前記所定の演算値を減算／加算する第２の演算処理手段と、

前記第２の演算処理手段において減算／加算されたバイトデータをデジタルデータに変換し、変換されたデジタルデータに対して、前記データ圧縮規格に基づいてデータ解凍処理を施すデータ解凍手段と、

を備えたことを特徴とするモデム装置。

【請求項１１】　前記第１および第２の演算処理手段は、所定のデータパタ

ーンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする請求項１０に記載のモデム装置。

【請求項１２】　さらに、前記所定の数値または所定のバイトコードに関する情報と、前記所定数に関する情報と、前記所定の演算値に関する情報と、を記憶する記憶手段と、

前記記憶手段によって記憶された前記所定の数値または所定のバイトコードに関する情報、前記所定数に関する情報、前記所定の演算値に関する情報のうちの少なくとも一つを変更する情報変更手段と、

を備えたことを特徴とする請求項１０または１１に記載のモデム装置。

【請求項１３】　データ送信装置と、前記データ送信装置によって送信されたデータを受信するデータ受信装置と、から構成されるデータ通信システムにおいて、

前記データ送信装置が、

送信するデータを順次読み込み、読み込まれたデータが所定の数値のデジタルデータを含んでいるか否かを判定する第１の判定処理手段と、

前記第１の判定処理手段によって、前記データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算／減算する第１の演算処理手段と、

前記第１の演算処理手段によって演算処理されたデータを送信する送信手段と、

を備え、

前記データ受信装置が、

前記データ送信装置によって送信されたデータを受信する受信手段と、

前記受信手段によって受信されたデータを順次読み込み、読み込まれたデータが前記所定の数値のデジタルデータを含んでいるか否かを判定する第２の判定処理手段と、

前記第２の判定処理手段によって、前記データが所定の数値のデジタルデータ

を含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する前記所定数のデジタルデータの全部または一部に対して、前記所定の演算値を減算／加算する第２の演算処理手段と、

を備えたことを特徴とするデータ通信システム。

【請求項１４】　データ送信装置と、前記データ送信装置によって送信されたデータを受信するデータ受信装置と、から構成されるデータ通信システムにおいて、

前記データ送信装置が、

シリアル入力されたバイナリデータである送信データをバイトデータに変換して一時的に保持する第１の保持手段と、

前記第１の保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第１の判定処理手段と、

前記第１の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第１の演算処理手段と、

前記第１の演算処理手段によって加算／除算されたバイトデータをバイナリデータに変換して送信する送信手段と、

を備え、

前記データ受信装置が、

シリアル入力されたバイナリデータである受信データをバイトデータに変換して一時的に保持する第２の保持手段と、

前記第２の保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第２の判定処理手段と、

前記第２の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第２の演算処理手段と、

前記第２の演算処理手段において減算／加算されたバイトデータをバイナリデータに変換する変換してシリアル出力する出力手段と、

を備えたことを特徴とするデータ送信システム。

【請求項１５】　前記データ送信装置と前記データ受信装置は、インターネットなどのネットワークによって互いに接続されていることを特徴とする請求項１３または１４に記載のデータ通信システム。

【請求項１６】　前記第１および第２の演算処理手段は、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする請求項１３～１５のいずれか一つに記載のデータ通信システム。

【請求項１７】　さらに、前記データ送信装置および前記データ受信装置が

前記所定の数値または所定のバイトコードに関する情報と、前記所定数に関する情報と、前記所定の演算値に関する情報と、を記憶する記憶手段と、

前記記憶手段によって記憶された前記所定の数値または所定のバイトコードに関する情報、前記所定数に関する情報、前記所定の演算値に関する情報のうちの少なくとも一つを、前記データ送信装置と前記データ受信装置とを同期させて変更する情報変更手段と、

を備えたことを特徴とする請求項１３～１６のいずれか一つに記載のデータ通信システム。

【請求項１８】　連続するデジタルデータを順次読み込む読込工程と、

前記読込工程によって読み込まれたデジタルデータが所定の連続パターンの数値であるか否かを判定する判定処理工程と、

前記判定処理工程によって判定された結果、前記所定の連続パターンの数値であると判定されたデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算または減算する演算処理工程と、

を含んだことを特徴とするデータ防護処理方法。

【請求項１９】　シリアル入力されたバイナリデータをバイトデータに変換して順次読み込む読込工程と、

前記読込工程によって読み込まれたバイトデータが所定のバイトコードであるか否かを判定する判定処理工程と、

前記判定処理工程によって判定された結果、前記所定のバイトコードであると

判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算または減算する演算処理工程と、

前記演算処理工程によって演算されたバイトデータをバイナリデータに変換してシリアル出力する出力工程と、

を含んだことを特徴とするデータ防護処理方法。

【請求項２０】　シリアル入力されたバイナリデータをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する保持工程と、

前記保持工程によって保持された所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出するデータ抽出処理工程と、

前記データ抽出処理工程から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する判定処理工程と、

前記判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算または減算する演算処理工程と、

前記演算処理工程によって演算されたバイトデータをもちいて前記所定のデータフレームを再構成するデータフレーム再構成処理工程と、

前記データフレーム再構成処理工程によって再構成されたデータフレームをバイナリデータに変換してシリアル出力する出力工程と、

を含んだことを特徴とするデータ防護処理方法。

【請求項２１】　前記演算処理工程は、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする請求項１８～２０のいずれか一つに記載のデータ防護処理方法。

【請求項２２】　連続するデジタルデータである送信データ／受信データを順次読み込む読込工程と、

前記読込工程によって読み込まれた送信データ／受信データが所定の数値のデジタルデータを含んでいるか否かを判定する第１の判定処理工程と、

前記第１の判定処理工程によって、前記送信データ／受信データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算／減算する第１の演算処理工程と、

連続するデジタルデータである受信データ／送信データを順次読み込み、読み込まれた受信データ／送信データが前記所定の数値のデジタルデータを含んでいるか否かを判定する第２の判定処理工程と、

前記第２の判定処理工程によって、前記受信データ／送信データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する前記所定数のデジタルデータの全部または一部に対して、前記所定の演算値を減算／加算する第２の演算処理工程と、

を含んだことを特徴とするデータ防護処理方法。

【請求項２３】　シリアル入力されたバイナリデータである送信データ／受信データをバイトデータに変換して順次読み込む第１の読込工程と、

前記第１の読込工程によって読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第１の判定処理工程と、

前記第１の判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第１の演算処理工程と、

前記第１の演算処理工程によって加算／除算されたバイトデータをバイナリデータに変換して送信データ／受信データとしてシリアル出力する第１の出力工程と、

シリアル入力されたバイナリデータである受信データ／送信データをバイトデータに変換して順次読み込む第２の読込工程と、

前記第２の読込工程によって読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第２の判定処理工程と、

前記第２の判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第２の演算処理工程と、

前記第２の演算処理工程において減算／加算されたバイトデータをバイナリデータに変換して受信データ／送信データとしてシリアル出力する第２の出力工程と、

を含んだことを特徴とするデータ防護処理方法。

【請求項２４】　シリアル入力されたバイナリデータである送信データ／受信データをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する第１の保持工程と、

前記第１の保持工程から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出する第１のデータ抽出処理工程と、

前記第１のデータ抽出処理工程から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第１の判定処理工程と、

前記第１の判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第１の演算処理工程と、

前記第１の演算処理工程によって加算されたバイトデータをもちいて前記所定のデータフレームを再構成する第１のデータフレーム再構成処理工程と、

前記第１のデータフレーム再構成処理工程によって再構成されたデータフレームをバイナリデータに変換して送信データ／受信データとしてシリアル出力する第１の出力工程と、

シリアル入力されたバイナリデータである受信データ／送信データをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する第２の保持工程と、

前記第２の保持工程から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出する第２のデータ抽出処理工程と、

前記第２のデータ抽出処理工程から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第２の判定処理工程と、

前記第２の判定処理工程によって判定された結果、前記所定のバイトコードで

あると判定されたバイトデータの後に連続する前記所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第２の演算処理工程と、

前記第２の演算処理工程において減算／加算されたバイトデータをもちいてデータフレームを再構成する第２のデータフレーム再構成処理工程と、

前記第２のデータフレーム再構成処理工程によって再構成されたデータフレームをバイナリデータに変換して受信データ／送信データとしてシリアル出力する第２の出力工程と、

を含んだことを特徴とするデータ防護処理方法。

【請求項２５】　前記第１および第２の演算処理工程は、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする請求項２２～２４のいずれか一つに記載のデータ防護処理方法。

【請求項２６】　さらに、前記所定の数値または所定のバイトコードに関する情報、前記所定数に関する情報、前記所定の演算値に関する情報のうちの少なくとも一つを変更する情報変更工程を含んだことを特徴とする請求項１８～２５のいずれか一つに記載のデータ防護処理方法。

【請求項２７】　前記請求項１８～２６のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、社内ＬＡＮを管理するシステム管理者が、そのＬＡＮに属しかつインターネット上で公開されたサーバにアクセスする際に、アクセス時および通信確立後の送受信データを、システム管理者が使用するクライアントとサーバとの間のみで符号化／復号化することによって、システム管理者のみに与えられたアクセス権限を保護することが可能なデータ防護処理装置、モデム装置、データ通信システム、データ防護処理方法、その方法をコンピュータに実行させるプロ

グラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【０００２】

【従来の技術】

インターネットは、オープンなネットワークであるがゆえに、自分が送信したデータが第三者に盗み見される可能性が大きいという問題を有している。そこで、インターネットの一般的な通信形態であるＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）サーバとＷＷＷブラウザとの間の通信においては、クレジット・カード番号などの保安性の要するデータを安全に送信したり、メールの送信者や内容が偽造されたりしていないことを証明するために、暗号化技術が導入されている。

【０００３】

この暗号化技術の代表的なものとしては、共通鍵暗号法と公開鍵暗号法が知られている。共通鍵暗号法とは、自分と相手が同じ暗号鍵を使って暗号化と復号化をおこなう方法である。一方、公開鍵暗号法は、現在主流となっている暗号方法である。秘密鍵と公開鍵という二つの鍵ペアをもちいて暗号化と復号化をおこない、どちらか一方の鍵で暗号化したデータは、もう一方の鍵を使わないと復号化できないという特徴を有している。

【０００４】

この公開鍵暗号法において、秘密鍵は、所持者（使用権限のある者）だけが自由に使うことができるため、自身で安全に管理する必要がある。一方、公開鍵は、ＷＷＷ上等で広く公開されており、誰でも取得して利用することができる。すなわち、秘密鍵を使ってデータを暗号化し、そのデータをペアとなる公開鍵で復号化することで、確かにそのデータが秘密鍵保持者によって暗号化されたことを確認できるという有効な利用が可能になる。この公開鍵暗号法の性質を活用したのが、いわゆる電子署名である。

【０００５】

また、ＷＷＷサーバとＷＷＷブラウザとの間における代表的な暗号化方式としては、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）が知られている。このＳＳＬは、上記した共通鍵暗号法と公開鍵暗号法とを組み合わせ、両暗号法の利点を生かしたものである。

【０００６】

特に、社内ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）等の社内ネットワークでは、専用線等の新たな通信インフラを整備するためのコストが不要になることから、公衆回線と上記した暗号化技術とを利用した、いわゆるＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）を構築した例が数多くある。

【０００７】

また、社内ＬＡＮでは、さらなるデータの保安性を図るために、ファイアウオールとして、社内クライアントのインターネット・アクセスを代行するプロキシサービスを導入している場合が多い。プロキシサービスは、社内ネットワークに配置されたプロキシサーバが、社内クライアントからのアクセス要求を受け取ると、それを解釈してインターネット上に存在する目的のサーバにアクセスし、結果を受け取って社内クライアントに渡す仕組みである。

【０００８】

この仕組みによって、インターネットからはプロキシサーバだけが見え、社内のマシンはまったく見えない。一方、社内クライアントが直接通信する相手はプロキシサーバだけであり、インターネット上のサーバと直接通信することはない。これによって、社内ＬＡＮにおいて、外部に対するデータの機密化が図られる。なお、ルータやゲートウェイが、プロキシサーバの機能を有している場合も多い。

【０００９】

一方、社内ＬＡＮ等のシステム管理者は、社内ＬＡＮに直接に接続されたクライアントからではなく、社外から社内ＬＡＮにアクセスし、サーバを管理することがある。社外からの社内ＬＡＮへのアクセスは、一般に、公衆回線を介しておこなわれるが、社内ＬＡＮ内に設置されたアクセスサーバにアクセスする方法（以下、直接アクセス方法と称する。）と、インターネット・サービス・プロバイダのアクセスサーバに接続した後にインターネット経由で社内ＬＡＮのＷＷＷサーバ等にアクセスする方法（以下、インターネットアクセス方法と称する。）とが知られている。

【００１０】

直接アクセス方法では、まず、システム管理者が、ノートパソコン等のクライアント・マシンをもちい、公衆回線を介して社内ＬＡＮのアクセスサーバに対してダイヤルアップ接続をおこなう。アクセスサーバは、社内ＬＡＮのメインサーバに接続されている。システム管理者は、このアクセスサーバを経由して、社内ＬＡＮ内の各種サーバにアクセスすることが可能になる。ここで、各種サーバとしては、コミュニケーションサーバはもちろんのこと、ＤＮＳ（Ｄｏｍａｉｎ Ｎａｍｅ　Ｓｙｓｔｅｍ）サーバ、メールサーバ、WWWサーバ等のインターネット標準プロトコルにしたがったサービスを享受するためのサーバである。

【００１１】

また、インターネットアクセス方法では、まず、システム管理者が、ノートパソコン等のクライアント・マシンをもちい、公衆回線を介してインターネット・サービス・プロバイダのアクセスサーバに対してダイヤルアップ接続をおこなう。インターネット・サービス・プロバイダのアクセスサーバは、ルータを介してインターネットのバックボーンに接続されている。このため、システム管理者は、このアクセスサーバを経由して、インターネットに接続することが可能になる。

【００１２】

インターネットに接続された後は、社内ＬＡＮの各種サーバのうち、バリア・セグメントに位置するサーバ、すなわちインターネット上に公開されたWWWサーバ等のサーバにアクセスする。この際、システム管理者は、たとえばWWWサーバ内の特別なWWWページにアクセスしたり、WWWサーバにアクセスした際に最初に表示されるホームページ上で特別なコマンドを入力することによって、WWWサーバが保持する各種ファイルを管理することができる。

【００１３】

【発明が解決しようとする課題】

しかしながら、上記したＶＰＮでは、社外から、公衆回線を介して社内ＬＡＮにアクセスする際およびアクセス後の送受信において、通信データのすべてに暗号化／復号化処理を施す必要がある。クライアントおよびサーバにおいて、それら処理による負荷の増大は無視できるものではない。特に、保安性を高めようと

すると、暗号化／復号化に要する演算が複雑になる。このため、より高速処理が可能なクライアントおよびサーバを選定する必要がある。これは、ＶＰＮの構築にあたってコスト増を意味する。

【００１４】

また、暗号化されたデータは、暗号化前のデータと比較してサイズが大きくなってしまうため、電子メールのように比較的サイズの小さなデータの送受信は問題とならない。しかし、大きなサイズのファイルを送受信する場合には、暗号化／復号化処理に時間を多く費やしてしまう。これは、暗号化／復号化処理が、送受信の対象となるデータ全体をすべて受け取った後で、そのデータ全体に対して一度に施される処理であることに起因する。このようなＶＰＮの問題は、システム管理者が社内ＬＡＮにアクセスする場合も例外ではない。

【００１５】

また、上記した直接アクセス方法では、社内ＬＡＮのアクセスサーバにアクセスした際に、一般にＩＤ番号とパスワードの入力が要求され、権限なき者のアクセスは拒絶される。しかし、アクセスサーバのダイヤル番号が知られている場合には、システム管理者以外であっても、そのようなＩＤ番号とパスワードの入力を求める状態に移行させることができる。これは、ＩＤ番号とパスワードを知らなくても、適当に入力した番号やアルファベットが上記したＩＤ番号とパスワードに一致する可能性を否定できない。

【００１６】

特に、クラッカー等の悪質な侵入者は、番号やアルファベットのあらゆる組み合わせを自動生成かつ自動入力するツールをもちいて、上記したＩＤ番号とパスワードとによる認証を解除しようとする。したがって、従来の直接アクセス方法では、上記したツールをもちいることで、システム管理者のなりすましが可能となってしまう。システム管理者は、一般に、企業の機密データを含めたほとんどすべてのデータを入手する権限が与えられている。このため、システム管理者のなりすましに対しては、これらデータが外部に漏洩することを防ぐことはできない。

【００１７】

一方、上記したインターネットアクセス方法においても、ＩＤ番号とパスワードの入力要求は直接アクセス方法の場合と共通であり、システム管理者のなりすましを完全に防ぐことは困難である。特に、社内のバリア・セグメント上のサーバは、インターネットの公開性の高さから、制限なくアクセスされることを前提にしている。したがって、システム管理用の特別なＷＷＷページやシステム管理モードに移行するための方法が知られてしまう可能性は高い。これは、システム管理用のＩＤ番号やパスワードの入力要求状態へと辿りついてしまうことを意味し、結局は、システム管理者のなりすましの問題へとつながる。

【００１８】

さらに、以上に説明した従来のＶＰＮ、直接アクセス方法およびインターネットアクセス方法は、いずれもアプリケーション層レベルにおいて、データ保安を実現しようとするものである。これは、特別な機器を必要とせずとも、コンピュータ・プログラムの知識を有していれば、比較的容易に、データ保安の打破が可能となることを意味する。すなわち、従来のデータ保安技術では、コスト的にも時間的にも、不正侵入者が有利な立場にある。

【００１９】

この発明は、上記に鑑みてなされたものであって、システム管理者が、社内ＬＡＮのサーバにアクセスする場合に、送受信データを、そのデータ・サイズを増大させることなく、システム管理者のみに与えられたアクセス権限を保護することを可能にしたデータ防護処理装置、モデム装置、データ防護処理方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【００２０】

【課題を解決するための手段】

上記の目的を達成するために、請求項１に記載の発明にかかるデータ防護処理装置にあっては、連続するデジタルデータを順次読み込み、読み込まれたデジタルデータが所定の連続パターンの数値であるか否かを判定する判定処理手段と、

前記判定処理手段によって判定された結果、前記所定の連続パターンの数値であると判定されたデジタルデータの後に連続する所定数のデジタルデータの全部

または一部に対して、所定の演算値を加算または減算する演算処理手段と、を備えたことを特徴とする。

【００２１】

また、請求項２に記載の発明にかかるデータ防護処理装置は、シリアル入力されたバイナリデータをバイトデータに変換して一時的に保持する保持手段と、前記保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する判定処理手段と、前記判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算または減算する演算処理手段と、前記演算処理手段によって演算されたバイトデータをバイナリデータに変換してシリアル出力する出力手段と、を備えたことを特徴とする。

【００２２】

また、請求項３に記載の発明にかかるデータ防護処理装置は、シリアル入力されたバイナリデータをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する保持手段と、前記保持手段から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出するデータ抽出処理手段と、前記データ抽出処理手段から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する判定処理手段と、前記判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算または減算する演算処理手段と、前記演算処理手段によって演算されたバイトデータをもちいて前記所定のデータフレームを再構成するデータフレーム再構成処理手段と、前記データフレーム再構成処理手段によって再構成されたデータフレームをバイナリデータに変換してシリアル出力する出力手段と、を備えたことを特徴とする。

【００２３】

また、請求項４に記載の発明にかかるデータ防護処理装置は、請求項１～３の

いずれか一つに記載の発明において、前記演算処理手段が、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする。

【００２４】

また、請求項５に記載の発明にかかるデータ防護処理装置は、連続するデジタルデータである送信データ／受信データを順次読み込み、読み込まれた送信データ／受信データが所定の数値のデジタルデータを含んでいるか否かを判定する第１の判定処理手段と、前記第１の判定処理手段によって、前記送信データ／受信データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算／減算する第１の演算処理手段と、連続するデジタルデータである受信データ／送信データを順次読み込み、読み込まれた受信データ／送信データが前記所定の数値のデジタルデータを含んでいるか否かを判定する第２の判定処理手段と、前記第２の判定処理手段によって、前記受信データ／送信データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する前記所定数のデジタルデータの全部または一部に対して、前記所定の演算値を減算／加算する第２の演算処理手段と、を備えたことを特徴とする。

【００２５】

また、請求項６に記載の発明にかかるデータ防護処理装置は、シリアル入力されたバイナリデータである送信データ／受信データをバイトデータに変換して一時的に保持する第１の保持手段と、前記第１の保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第１の判定処理手段と、前記第１の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第１の演算処理手段と、前記第１の演算処理手段によって加算／除算されたバイトデータをバイナリデータに変換して送信データ／受信データとしてシリアル出力する第１の出力手段と、シリアル入力されたバイナリデータである受信データ／送

信データをバイトデータに変換して一時的に保持する第２の保持手段と、前記第２の保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第２の判定処理手段と、前記第２の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第２の演算処理手段と、前記第２の演算処理手段において減算／加算されたバイトデータをバイナリデータに変換して受信データ／送信データとしてシリアル出力する第２の出力手段と、を備えたことを特徴とする。

【００２６】

また、請求項７に記載の発明にかかるデータ防護処理装置は、シリアル入力されたバイナリデータである送信データ／受信データをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する第１の保持手段と、前記第１の保持手段から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出する第１のデータ抽出処理手段と、

前記第１のデータ抽出処理手段から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第１の判定処理手段と、前記第１の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第１の演算処理手段と、前記第１の演算処理手段によって加算されたバイトデータをもちいて前記所定のデータフレームを再構成する第１のデータフレーム再構成処理手段と、前記第１のデータフレーム再構成処理手段によって再構成されたデータフレームをバイナリデータに変換して送信データ／受信データとしてシリアル出力する第１の出力手段と、シリアル入力されたバイナリデータである受信データ／送信データをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する第２の保持手段と、前記第２の保持手段から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出する第２のデータ抽出処理手段と、前記第２のデータ抽出処理手

段から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第２の判定処理手段と、前記第２の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する前記所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第２の演算処理手段と、前記第２の演算処理手段において減算／加算されたバイトデータをもちいてデータフレームを再構成する第２のデータフレーム再構成処理手段と、前記第２のデータフレーム再構成処理手段によって再構成されたデータフレームをバイナリデータに変換して受信データ／送信データとしてシリアル出力する第２の出力手段と、を備えたことを特徴とする。

【００２７】

また、請求項８に記載の発明にかかるデータ防護処理装置は、請求項５～７のいずれか一つに記載の発明において、前記第１および第２の演算処理手段が、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする。

【００２８】

また、請求項９に記載の発明にかかるデータ防護処理装置は、請求項１～８のいずれか一つに記載の発明において、さらに、前記所定の数値または所定のバイトコードに関する情報と、前記所定数に関する情報と、前記所定の演算値に関する情報と、を記憶する記憶手段と、前記記憶手段によって記憶された前記所定の数値または所定のバイトコードに関する情報、前記所定数に関する情報、前記所定の演算値に関する情報のうちの少なくとも一つを変更する情報変更手段と、を備えたことを特徴とする。

【００２９】

また、請求項１０に記載の発明にかかるモデム装置は、送信するデジタルデータに対して、標準化されたデータ圧縮規格に基づいてデータ圧縮処理を施すデータ圧縮手段と、前記データ圧縮手段によってデータ圧縮処理を施されたデジタルデータをバイトデータに変換し、変換されたバイトデータを順次読み込み、読み

込まれたバイトデータが所定のバイトコードであるか否かを判定する第１の判定処理手段と、前記第１の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して所定の演算値を加算／減算する第１の演算処理手段と、前記第１の演算処理手段において加算／減算されたバイトデータを出力する第１の出力手段と、受信したデジタルデータをバイトデータに変換し、変換されたバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第２の判定処理手段と、前記第２の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して前記所定の演算値を減算／加算する第２の演算処理手段と、前記第２の演算処理手段において減算／加算されたバイトデータをデジタルデータに変換し、変換されたデジタルデータに対して、前記データ圧縮規格に基づいてデータ解凍処理を施すデータ解凍手段と、を備えたことを特徴とする。

【００３０】

また、請求項１１に記載の発明にかかるモデム装置は、請求項１０に記載の発明において、前記第１および第２の演算処理手段が、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする。

【００３１】

また、請求項１２に記載の発明にかかるモデム装置は、請求項１０または１１に記載の発明において、さらに、前記所定の数値または所定のバイトコードに関する情報と、前記所定数に関する情報と、前記所定の演算値に関する情報と、を記憶する記憶手段と、前記記憶手段によって記憶された前記所定の数値または所定のバイトコードに関する情報、前記所定数に関する情報、前記所定の演算値に関する情報のうちの少なくとも一つを変更する情報変更手段と、を備えたことを特徴とする。

【００３２】

また、請求項１３に記載の発明にかかるデータ通信システムは、データ送信装

置と、前記データ送信装置によって送信されたデータを受信するデータ受信装置と、から構成されるデータ通信システムにおいて、前記データ送信装置が、送信するデータを順次読み込み、読み込まれたデータが所定の数値のデジタルデータを含んでいるか否かを判定する第１の判定処理手段と、前記第１の判定処理手段によって、前記データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算／減算する第１の演算処理手段と、前記第１の演算処理手段によって演算処理されたデータを送信する送信手段と、を備え、前記データ受信装置が、前記データ送信装置によって送信されたデータを受信する受信手段と、前記受信手段によって受信されたデータを順次読み込み、読み込まれたデータが前記所定の数値のデジタルデータを含んでいるか否かを判定する第２の判定処理手段と、前記第２の判定処理手段によって、前記データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する前記所定数のデジタルデータの全部または一部に対して、前記所定の演算値を減算／加算する第２の演算処理手段と、を備えたことを特徴とする。

【００３３】

また、請求項１４に記載の発明にかかるデータ通信システムは、データ送信装置と、前記データ送信装置によって送信されたデータを受信するデータ受信装置と、から構成されるデータ通信システムにおいて、前記データ送信装置が、シリアル入力されたバイナリデータである送信データをバイトデータに変換して一時的に保持する第１の保持手段と、前記第１の保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第１の判定処理手段と、前記第１の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第１の演算処理手段と、前記第１の演算処理手段によって加算／除算されたバイトデータをバイナリデータに変換して送信する送信手段と、を備え、前記データ受信装置が、シリアル入力されたバイナリデータである受信データをバイトデータに変

換して一時的に保持する第２の保持手段と、前記第２の保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第２の判定処理手段と、前記第２の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第２の演算処理手段と、前記第２の演算処理手段において減算／加算されたバイトデータをバイナリデータに変換する変換してシリアル出力する出力手段と、を備えたことを特徴とする。

【００３４】

また、請求項１５に記載の発明にかかるデータ通信システムは、請求項１３または１４に記載の発明において、前記データ送信装置と前記データ受信装置が、インターネットなどのネットワークによって互いに接続されていることを特徴とする。

【００３５】

また、請求項１６に記載の発明にかかるデータ通信システムは、請求項１３～１５のいずれか一つに記載の発明において、前記第１および第２の演算処理手段が、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする。

【００３６】

また、請求項１７に記載の発明にかかるデータ通信システムは、請求項１３～１６のいずれか一つに記載の発明において、さらに、前記データ送信装置および前記データ受信装置が、前記所定の数値または所定のバイトコードに関する情報と、前記所定数に関する情報と、前記所定の演算値に関する情報と、を記憶する記憶手段と、前記記憶手段によって記憶された前記所定の数値または所定のバイトコードに関する情報、前記所定数に関する情報、前記所定の演算値に関する情報のうちの少なくとも一つを、前記データ送信装置と前記データ受信装置とを同期させて変更する情報変更手段と、を備えたことを特徴とする。

【００３７】

また、請求項１８に記載の発明にかかるデータ防護処理方法は、連続するデジタルデータを順次読み込む読込工程と、前記読込工程によって読み込まれたデジタルデータが所定の連続パターンの数値であるか否かを判定する判定処理工程と、前記判定処理工程によって判定された結果、前記所定の連続パターンの数値であると判定されたデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算または減算する演算処理工程と、を含んだことを特徴とする。

【００３８】

また、請求項１９に記載の発明にかかるデータ防護処理方法は、シリアル入力されたバイナリデータをバイトデータに変換して順次読み込む読込工程と、前記読込工程によって読み込まれたバイトデータが所定のバイトコードであるか否かを判定する判定処理工程と、前記判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算または減算する演算処理工程と、前記演算処理工程によって演算されたバイトデータをバイナリデータに変換してシリアル出力する出力工程と、を含んだことを特徴とする。

【００３９】

また、請求項２０に記載の発明にかかるデータ防護処理方法は、シリアル入力されたバイナリデータをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する保持工程と、前記保持工程によって保持された所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出するデータ抽出処理工程と、前記データ抽出処理工程から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する判定処理工程と、前記判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算または減算する演算処理工程と、前記演算処理工程によって演算されたバイトデータをもちいて前記所定のデータフレームを再構成するデータフレーム再構成処理工程と、前記データフレーム再構成処理工程によって再構成された

データフレームをバイナリデータに変換してシリアル出力する出力工程と、を含んだことを特徴とする。

【００４０】

また、請求項２１に記載の発明にかかるデータ防護処理方法は、請求項１８～２０のいずれか一つに記載の発明のおいて、前記演算処理工程が、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする。

【００４１】

また、請求項２２に記載の発明にかかるデータ防護処理方法は、連続するデジタルデータである送信データ／受信データを順次読み込む読込工程と、前記読込工程によって読み込まれた送信データ／受信データが所定の数値のデジタルデータを含んでいるか否かを判定する第１の判定処理工程と、前記第１の判定処理工程によって、前記送信データ／受信データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算／減算する第１の演算処理工程と、連続するデジタルデータである受信データ／送信データを順次読み込み、読み込まれた受信データ／送信データが前記所定の数値のデジタルデータを含んでいるか否かを判定する第２の判定処理工程と、前記第２の判定処理工程によって、前記受信データ／送信データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する前記所定数のデジタルデータの全部または一部に対して、前記所定の演算値を減算／加算する第２の演算処理工程と、を含んだことを特徴とする。

【００４２】

また、請求項２３に記載の発明にかかるデータ防護処理方法は、シリアル入力されたバイナリデータである送信データ／受信データをバイトデータに変換して順次読み込む第１の読込工程と、前記第１の読込工程によって読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第１の判定処理工程と、前記第１の判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または

一部に対して、所定の演算値を加算／除算する第１の演算処理工程と、前記第１の演算処理工程によって加算／除算されたバイトデータをバイナリデータに変換して送信データ／受信データとしてシリアル出力する第１の出力工程と、シリアル入力されたバイナリデータである受信データ／送信データをバイトデータに変換して順次読み込む第２の読込工程と、前記第２の読込工程によって読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第２の判定処理工程と、前記第２の判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第２の演算処理工程と、前記第２の演算処理工程において減算／加算されたバイトデータをバイナリデータに変換して受信データ／送信データとしてシリアル出力する第２の出力工程と、を含んだことを特徴とする。

【００４３】

また、請求項２４に記載の発明にかかるデータ防護処理方法は、シリアル入力されたバイナリデータである送信データ／受信データをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する第１の保持工程と、前記第１の保持工程から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出する第１のデータ抽出処理工程と、前記第１のデータ抽出処理工程から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第１の判定処理工程と、前記第１の判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第１の演算処理工程と、前記第１の演算処理工程によって加算されたバイトデータをもちいて前記所定のデータフレームを再構成する第１のデータフレーム再構成処理工程と、前記第１のデータフレーム再構成処理工程によって再構成されたデータフレームをバイナリデータに変換して送信データ／受信データとしてシリアル出力する第１の出力工程と、シリアル入力されたバイナリデータである受信データ／送信データをバイトデータに変換し、変換されたバイトデータを所定

のデータフレームごとに一時的に保持する第２の保持工程と、前記第２の保持工程から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出する第２のデータ抽出処理工程と、前記第２のデータ抽出処理工程から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第２の判定処理工程と、前記第２の判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する前記所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第２の演算処理工程と、前記第２の演算処理工程において減算／加算されたバイトデータをもちいてデータフレームを再構成する第２のデータフレーム再構成処理工程と、前記第２のデータフレーム再構成処理工程によって再構成されたデータフレームをバイナリデータに変換して受信データ／送信データとしてシリアル出力する第２の出力工程と、を含んだことを特徴とする。

【００４４】

また、請求項２５に記載の発明にかかるデータ防護処理方法は、請求項２２～２４のいずれか一つに記載の発明のおいて、前記第１および第２の演算処理工程が、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする。

【００４５】

また、請求項２６に記載の発明にかかるデータ防護処理方法は、請求項１８～２５のいずれか一つに記載の発明のおいて、さらに、前記所定の数値または所定のバイトコードに関する情報、前記所定数に関する情報、前記所定の演算値に関する情報のうちの少なくとも一つを変更する情報変更工程を含んだことを特徴とする。

【００４６】

また、請求項２７に記載の発明にかかる記録媒体は、請求項１８～２６のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、当該プログラムをコンピュータによって読み取ることが可能となり、これ

によって、請求項９～１６の動作をコンピュータによって実現することが可能である。

【００４７】

【発明の実施の形態】

以下、この発明にかかるデータ防護処理装置、モデム装置およびデータ防護処理方法の好適な実施の形態について添付図面を参照し、詳細に説明する。なお、この実施の形態によってこの発明が限定されるものではない。

【００４８】

（実施の形態１）

まず、実施の形態１にかかるデータ防護処理装置およびデータ防護処理方法について説明する。実施の形態１にかかるデータ防護処理装置およびデータ防護処理方法は、シリアル入力されるビットデータ列に対してバイト変換をおこなうことでバイト列を取得する。そして、取得したバイト列に含まれる所定のバイトデータの存在を条件として、バイトコードから所定範囲にわたるバイトデータに対して所定の防護キー値を加算することで符号化をおこなうことを特徴としている。また、逆の手順によって復号化をおこなうことも特徴とする。

【００４９】

図１は、実施の形態１にかかるデータ防護処理装置の概略構成を示すブロック図である。図１に示すデータ防護処理装置１０は、通信回線上や通信機器へと送信しようとする送信データに対して符号化処理を施す符号化処理部と、通信回線上や通信機器から受信した受信データに対して復号化処理を施す復号化処理部と、付加条件／付加範囲／防護キー記憶部３０と、を備えて構成される。

【００５０】

まず、付加条件／付加範囲／防護キー記憶部３０は、付加条件、付加範囲および防護キー値を記憶するものである。ここで、付加条件とは、バイトデータが、どのバイトコードを示した場合にそのバイトデータからいくつ後のバイトデータに対して防護キー値の加算をおこなうかを示すものである。したがって、この付加条件は、所定のバイトコードと加算開始位置を示す数値とから構成される。

【００５１】

また、付加範囲とは、付加条件によって示される加算開始位置から、いくつのバイトデータにわたって防護キー値を加算するかを示すものであり、その範囲を示す数値によって表わされる。防護キー値とは、上記したように、バイトデータに加算する数値を表わすものである。

【００５２】

また、付加条件／付加範囲／防護キー記憶部３０に記憶される付加条件、付加範囲および防護キー値は、外部より書き換え可能にすることもできる。たとえば、インターネット上の時刻サーバやＧＰＳ（Ｇｌｏｂａｌ　Ｐｏｉｎｔｉｎｇ　Ｓｙｓｔｅｍ）衛星の原子時計に同期して、一斉に防護キー値を所定の値に変更するといった形態を採用することができる。これによって、より強固なデータ保安を図ることが可能になる。

【００５３】

また、データの送信側から付加条件、付加範囲および防護キー値に関する情報を取得して、その情報に基づいて、操作者が図示を省略するキーボードなどをもちいて書き換えることもできる。その際、あらかじめ図示を省略する変換テーブルを備え、数字または記号により書かれたデータを入力することによって、上記変換テーブルで付加条件、付加範囲および防護キー値に関するデータに変換して入力するようにしてもよい。このように送受信者間のみで独自の通信をおこなうことができる。

【００５４】

符号化処理部は、第１送信バッファ２２と、防護キー付加位置判定部２４と、防護キー付加処理部２６と、第２送信バッファ２８と、から構成される。第１送信バッファ２２は、外部から受け取ったデータ、特にシリアルビットデータを、少なくとも複数のバイトが構成できる容量分のデータを蓄積する記憶部である。また、この第１送信バッファ２２は、デジタルデータのシリアルーパラレル変換を可能としたＦＩＦＯ（Ｆｉｒｓｔ　Ｉｎ　Ｆｉｒｓｔ　Ｏｕｔ）メモリとしての機能を果たす。

【００５５】

防護キー付加位置判定部２４は、第１送信バッファに蓄積されたバイトデータ

をその蓄積順に取り出し、取り出したバイトデータが、上記した付加条件によって示されるバイトコードに一致するか否かを判定するものである。防護キー付加位置判定部２４は、第１送信バッファから取り出したバイトデータが上記付加条件を満たす場合には、たとえば、その旨を示す付加フラグをＯＮ状態にしたり、後述するように付加カウンタをカウントアップする。

【００５６】

防護キー付加処理部２６は、第１送信バッファか２２から取り出されたバイトデータを、防護キー付加位置判定部２４を介して受け取り、受け取ったバイトデータが上記付加条件を満たす場合に、そのバイトデータに上記防護キー値を加算する。具体的には、防護キー付加処理部２６は、上記付加フラグや付加カウンタの状態に応じて、バイトデータに対して防護キー値を加算するか否かを判定する。

【００５７】

第２送信バッファ２８は、防護キー付加処理部２６において付加処理が施されたバイトデータおよび付加処理が施されなかったバイトデータを蓄積する記憶部である。また、この第２送信バッファ２８は、デジタルデータのパラレルーシリアル変換を可能としたＦＩＦＯメモリとしての機能を果たす。したがって、符号化処理部は、第１送信バッファ２２が受け取ったデータに対し、所定の条件を満たすデータ部のみを変容させることになる。特に、その変容前後において、データサイズに変化がないことを特徴としている。

【００５８】

一方、復号化処理部は、第１受信バッファ３８と、防護キー除去位置判定部３６と、防護キー除去処理部３４と、第２受信バッファ３２と、から構成され、上述した符号化処理部と逆の処理をおこなう。第１受信バッファ３８は、上記した第１送信バッファと同様の機能を果たす記憶部である。

【００５９】

防護キー除去位置判定部３６は、第１受信バッファに蓄積されたバイトデータをその蓄積順に取り出し、取り出したバイトデータが、上記した付加条件によって示されるバイトコードに一致するか否かを判定するものである。防護キー除去

位置判定部３６は、第１受信バッファから取り出したバイトデータが上記付加条件を満たす場合には、たとえば、その旨を示す付加フラグをＯＮ状態にしたり、後述するように付加カウンタをカウントアップする。したがって、この防護キー除去位置判定部３６は、機能としては上記した防護キー付加位置判定部２４と同じであり、復号化処理部において防護キー除去位置判定部３６を設けずに、防護キー付加位置判定部２４を兼用してもよい。

【００６０】

防護キー除去処理部３４は、第１受信バッファ３８から取り出されたバイトデータを、防護キー除去位置判定部３６を介して受け取り、受け取ったバイトデータが上記付加条件を満たす場合に、そのバイトデータから上記防護キー値を差し引く。具体的には、防護キー除去処理部３４は、上記付加フラグや付加カウンタの状態に応じて、バイトデータに対して防護キー値を差し引くか否かを判定する。

【００６１】

第２受信バッファ３２は、防護キー除去処理部３４において除去処理が施されたバイトデータおよび除去処理が施されなかったバイトデータを蓄積する記憶部である。また、この第２受信バッファ３２は、デジタルデータのパラレルーシリアル変換を可能としたＦＩＦＯメモリとしての機能を果たす。したがって、復号化処理部は、第１受信バッファ３８が受け取ったデータに対し、所定の条件を満たすデータ部のみを変容させることになる。特に、上記した符号化処理部によって変容されたデータに対しては復号化処理を施すことになる。

【００６２】

したがって、データ防護処理装置１０から出力された送信データは、データ防護処理装置１０をもちいて受信しなければ、送信内容を正しく取得することはできない。すなわち、データ防護処理装置１０は、符号化／復号化処理を、付加条件／付加範囲／防護キー記憶部３０に記憶された内容にしたがってデータサイズを増減させることなく実行する装置である。

【００６３】

つぎに、このデータ防護処理装置１０の動作について、符号化処理および復号

化処理に分けて説明する。ここでは、説明を簡単にするために、上記した付加条件のうち加算開始位置を１とする。これは、付加条件によって示されるバイトコード、すなわち付加処理を実行するきっかけとなるバイトデータのつぎに位置するバイトデータから防護キー値の加算または減算をおこなうことを意味する。

【００６４】

まず、データ防護処理装置１０の符号化処理について説明する。図２は、実施の形態１にかかるデータ防護処理装置の符号化処理を示すフローチャートである。データ防護処理装置１０は、符号化処理を開始するにあたって、まず、符号化の対象となる送信データを第１送信バッファ２２に取りこむ。そして、防護キー付加位置判定部２４が、第１送信バッファ２２から１バイト分のデータを読み出す（ステップＳ２０１）。また、防護キー付加位置判定部２４は、自身が管理する付加カウンタが０より大きい値を示しているか否かを判定する（ステップＳ２０２）。

【００６５】

ステップＳ２０２において付加カウンタが０である場合には、防護キー付加位置判定部２４は、第１送信バッファ２２から読み出したバイトデータに対して付加処理を施す必要はないと判断し、現在読み出しているバイトデータが防護キー付加条件、すなわち上記したバイトコードと一致するか否かを判定する（ステップＳ２０７）。

【００６６】

ステップＳ２０７においてバイトデータが防護キー付加条件と一致しない場合には、防護キー付加位置判定部２４は、現在読み出しているバイトデータをそのまま次段の防護キー付加処理部２６に渡し、防護キー付加処理部２６は付加処理を実行することなく、そのバイトデータを第２送信バッファ２８に書き込む（ステップＳ２０９）。

【００６７】

ステップＳ２０７においてバイトデータが防護キー付加条件と一致する場合には、防護キー付加位置判定部２４は、上記した付加カウンタを１にセットし（ステップＳ２０８）、ステップＳ２０９の処理をおこなう。

【００６８】

ステップＳ２０２において付加カウンタが０より大きい場合には、防護キー付加位置判定部２４は、第１送信バッファ２２から読み出したバイトデータに対して付加処理を施す必要があると判断し、次段の防護キー付加処理部２６に、現在読み出しているバイトデータを渡すとともに、付加処理を依頼する。これによって、防護キー付加処理部２６は、受け取ったバイトデータに、付加条件／付加範囲／防護キー記憶部３０に記憶されている防護キー値を加算する（ステップＳ２０３）。

【００６９】

図３は、防護キー値の加算処理を説明するための説明図である。ステップＳ２０３における加算処理は、たとえば、図３に示すように、防護キー値がヘキサコード“１Ｅ”で表わされ、第１送信バッファ２２から読み出したデータがバイナリコードで“１０１１００１０”と表わされたバイトデータ、すなわちヘキサコード“Ｂ２”で表わされる場合、バイトデータ“Ｂ２”に防護キー値“１Ｅ”を加算することによりおこなう。したがって、この場合、加算結果として、バイナリコード“１１０１０００”と表わされたバイトデータ、すなわちヘキサコード“Ｄ０”を得ることができる。

【００７０】

防護キー付加位置判定部２４は、防護キー付加処理部２６による加算処理が終わると、または防護キー付加処理部２６に対して加算処理を依頼すると、付加カウンタが付加条件／付加範囲／防護キー記憶部３０に記憶されている付加範囲を超えているか否かを判定する（ステップＳ２０４）。

【００７１】

ステップＳ２０４において付加カウンタが付加範囲を超えていない場合は、防護キー付加位置判定部２４は、付加カウンタの値をインクリメントし（ステップＳ２０６）、ステップＳ２０９の処理をおこなう。一方、ステップＳ２０４において付加カウンタが付加範囲を超えている場合は、防護キー付加位置判定部２４は、付加カウンタの値をリセットし（ステップＳ２０５）、ステップＳ２０９の処理をおこなう。

【００７２】

以上の処理によって、データ防護処理装置１０は、第１送信バッファ２２に蓄積されたバイトデータに対し、付加条件／付加範囲／防護キー記憶部３０に記憶された諸条件にしたがった符号化を実現する。図４は、符号化処理によって得られるバイトデータ列の例を示す図である。

【００７３】

図４に示すように、付加条件がバイトコード“５Ｄ”のつぎからとし、防護キー値を“１Ｅ”、付加範囲を３とした場合には、データ防護処理装置１０の符号化処理によって、“５Ｄ　９Ｂ　１１　４０　Ａ９”の部分は、“５Ｄ　Ｂ９　２Ｆ　５Ｅ　Ａ９”に変容され、“５Ｄ　８８　ＦＡ　１Ｂ　３３”の部分は、“５Ｄ　Ａ６　１９　３９　３３”に変容される。ここで、“ＦＡ”から“１９”に変容されているように、防護キー値を加算した結果が、１バイトで表わされる数値範囲を超える場合には、その超えた部分の数値を加算結果とする。

【００７４】

また、上記の例においては、防護キー値を一種類のみ設定していたが、防護キー値を複数の値から構成されるデータパターンとして用意しておき、付加範囲の先頭から順に、そのデータパターンが順次示す値を、加算または減算するようにしてもよい。たとえば、図４に示した例で、付加条件および付加範囲は同じで、防護キー値を“１Ｅ，ＡＢ，７Ｆ”とすると、“５Ｄ”のつぎの“９Ｂ”に対して、“１Ｅ”を加算され、つぎの“１１”に対して“ＡＢ”を加算し、つぎの“４０”に対して“７Ｆ”を加算する。

【００７５】

また、付加条件、付加範囲の設定方法については、以下のような方法であってもよい。たとえば、付加条件を“５Ｄ”つぎとそのつぎをとばして３つ先からとし、付加範囲を一つおきに３バイトとする。それによって、図４に示した例をもちいると、加算の対象となるのは、（“９Ｂ”と“１１”をとばした３つ先の）“４０”と“ＤＤ”と“３８”ということになる。いずれにせよ、所定の数値のバイトデータの後に連続する所定数のバイトデータの全部または一部であれば、その内容についてはどのようなものであってもよい。

【００７６】

プログラムは、基本的には８ビットコードの配列として表現されており、そのソースでコマンド等を構成するアルファベットや数値を表わすのに、８ビットコードのうち７ビットしかもちいておらず、最上位ビットである８ビット目を“１”に置換すると、コンピュータ上で認識できないコードになる。したがって、対象のデータがプログラムである場合は、防護キー値として、８ビット目を“１”に置換するようなヘキサコードとして、“８０”～“ＦＦ”のいずれかをもちいるとより有効である。

【００７７】

つぎに、データ防護処理装置１０の復号化処理について説明する。図５は、実施の形態１にかかるデータ防護処理装置の復号化処理を示すフローチャートである。データ防護処理装置１０は、復号化処理を開始するにあたって、まず、復号化の対象となる受信データを第１受信バッファ３８に取りこむ。そして、防護キー除去位置判定部３６が、第１受信バッファ３８から１バイト分のデータを読み出す（ステップＳ５０１）。また、防護キー除去位置判定部３６は、自身が管理する付加カウンタが０より大きい値を示しているか否かを判定する（ステップＳ５０２）。

【００７８】

ステップＳ５０２において付加カウンタが０である場合には、防護キー除去位置判定部３６は、第１受信バッファ３８から読み出したバイトデータに対して除去処理を施す必要はないと判断し、現在読み出しているバイトデータが防護キー付加条件、すなわち上記したバイトコードと一致するか否かを判定する（ステップＳ５０７）。

【００７９】

ステップＳ５０７においてバイトデータが防護キー付加条件と一致しない場合には、防護キー除去位置判定部３６は、現在読み出しているバイトデータをそのまま次段の防護キー除去処理部３４に渡す。そして、防護キー除去処理部３４は除去処理を実行することなく、そのバイトデータを第２受信バッファ３２に書き込む（ステップＳ５０９）。

【００８０】

ステップＳ５０７においてバイトデータが防護キー付加条件と一致する場合には、防護キー除去位置判定部３６は、上記した付加カウンタを１にセットし（ステップＳ５０８）、ステップＳ５０９の処理をおこなう。

【００８１】

ステップＳ５０２において付加カウンタが０より大きい場合には、防護キー除去位置判定部３６は、第１受信バッファ３８から読み出したバイトデータに対して減算処理を施す必要があると判断し、次段の防護キー除去処理部３４に、現在読み出しているバイトデータを渡すとともに、減算処理を依頼する。これによって、防護キー除去処理部３４は、受け取ったバイトデータから、付加条件／付加範囲／防護キー記憶部３０に記憶されている防護キー値を差し引く（ステップＳ５０３）。なお、この減算処理は、図３に示した加算処理と逆の処理であるので、ここではその説明を省略する。

【００８２】

防護キー除去位置判定部３６は、防護キー除去処理部３４による減算処理が終わると、または防護キー除去処理部３４に対して減算処理を依頼すると、付加カウンタが付加条件／付加範囲／防護キー記憶部３０に記憶されている付加範囲を超えているか否かを判定する（ステップＳ５０４）。

【００８３】

ステップＳ５０４において付加カウンタが付加範囲を超えていない場合は、防護キー除去位置判定部３６は、付加カウンタの値をインクリメントし（ステップＳ５０６）、ステップＳ５０９の処理をおこなう。一方、ステップＳ５０４において付加カウンタが付加範囲を超えている場合は、防護キー除去位置判定部３６は、付加カウンタの値をリセットし（ステップＳ５０５）、ステップＳ５０９の処理をおこなう。

【００８４】

以上の処理によって、データ防護処理装置１０は、第１受信バッファ３８に蓄積されたバイトデータに対し、付加条件／付加範囲／防護キー記憶部３０に記憶された諸条件にしたがった復号化を実現する。

【００８５】

以上に説明したように、実施の形態１にかかるデータ防護処理装置およびデータ防護処理方法によれば、通信回線上や通信機器に送信しようとするシリアルデータをバイトごとに監視して、そのバイトデータが所定のバイトコードに一致しているか否かを判定し、一致している場合には、その一致箇所から所定の個数後に受け取ったバイトデータを開始位置として、その開始位置にあるバイトデータから所定の個数にわたるバイトデータに所定の値を加算することで符号化を実現しているので、データの符号化をデータサイズの変化なく実現することができる。

【００８６】

また、通信回線上や通信機器から受信したシリアルデータをバイトごとに監視して、そのバイトデータが所定のバイトコードに一致しているか否かを判定し、一致している場合には、その一致箇所から所定の個数後に受け取ったバイトデータを開始位置として、その開始位置にあるバイトデータから所定の個数にわたるバイトデータから所定の値を差し引くことで、上記した符号化に対応した復号化を実現することができる。

【００８７】

したがって、実施の形態１にかかるデータ防護処理装置およびデータ防護処理方法は、送受信する一連のデジタルコンテンツのデジタルデータのすべてを受け取らずとも、実際に受け取った部分から順に符号化／復号化処理を実行することが可能になるので、送信／受信バッファとして大容量のものを必要とすることなく、装置構成を安価にすることができる。

【００８８】

特に、このデータ防護処理装置を互いに有する二者間においては、データの機密化と高速な送受信をともに実現することができる。

【００８９】

なお、以上に説明した実施の形態１では、符号化処理において防護キー値を加算し、復号化処理において防護キー値を減算するとしたが、逆に、符号化処理において防護キー値を減算し、復号化処理において防護キー値を加算してもよい。

【００９０】

また、以上に説明した実施の形態１にかかるデータ防護処理装置において、付加条件／付加範囲／防護キー記憶部３０に記憶される付加条件、付加範囲および防護キー値は、外部より書き換え可能にすることもできる。

【００９１】

（実施の形態２）

つぎに、実施の形態２にかかるデータ防護処理装置およびデータ防護処理方法について説明する。実施の形態２は、実施の形態１にかかるデータ防護処理装置およびデータ防護処理方法を、上述した直接アクセス方法に適用した例を説明するものである。したがって、実施の形態１において説明した内容については同様であるのでその説明は省略する。

【００９２】

図６は、実施の形態２にかかるデータ防護処理装置およびデータ防護処理方法の適用例を示すシステム構成図である。図６においては、システム管理者の使用するクライアント１３０が公衆回線１４０を介して社内ＬＡＮ１２０のアクセスサーバ１２４に接続する場合を示している。

【００９３】

図６において、社内ＬＡＮ１２０は、専用線を介してインターネット・サービス・プロバイダ１１０に接続されており、インターネット・サービス・プロバイダ１１０は、ルータＲ１０をインターネット１００のバックボーンに接続している。これによって、社内ＬＡＮ１２０内のクライアント１２８は、ルータＲ２０を介して、インターネット１００に接続することが可能となっている。

【００９４】

図６において、直接アクセス方法に実施の形態１にかかるデータ防護処理装置およびデータ防護処理方法を適用するには、クライアント１３０側のＴＡ（ターミナルアダプタ）／モデムと、アクセスサーバ１２４側のＴＡ（ターミナルアダプタ）／モデムとに、それぞれ実施の形態１において説明したデータ防護処理方法を実現する機能を設ける。

【００９５】

クライアント１３０が社内ＬＡＮのアクセスサーバ１２４に接続する場合を考える。まず、クライアント１３０は、アクセスサーバ１２４にダイヤルすることでダイヤルアップ接続を確立する。

【００９６】

つづいてアクセスサーバ１２４は、ＩＤ番号／パスワード入力要求を示した送信データをデータ防護機能付ＴＡ／モデム１２６に出力する。そこで、送信データは、実施の形態１に説明した符号化処理を施されるとともに、公衆回線１４０の信号規格に応じて、アナログ変換や電圧変換の処理を施される。

【００９７】

これによって、符号化された送信データは、公衆回線１４０を介してデータ防護機能付ＴＡ／モデム１３２に到達し、そこで実施の形態１に説明した復号化処理が施される。復号化された送信データは、クライアント１３０において解釈され、その表示装置上にＩＤ番号／パスワード入力要求画面として表示される。

【００９８】

システム管理者は、ＩＤ番号／パスワード入力要求に対して、ＩＤ番号とパスワードを入力し、クライアント１３０は、入力されたＩＤ番号とパスワードを送信データとして、データ防護機能付ＴＡ／モデム１３２に出力する。そこで、送信データは、実施の形態１に説明した符号化処理を施されるとともに、公衆回線１４０の信号規格に応じて、アナログ変換や電圧変換の処理を施される。

【００９９】

これによって、符号化された送信データは、公衆回線１４０を介してデータ防護機能付ＴＡ／モデム１２６に到達し、そこで実施の形態１に説明した復号化処理が施される。復号化された送信データは、アクセスサーバ１２４において解釈され、アクセスが正規のシステム管理者によるものである否かの認証確認がおこなわれる。

【０１００】

アクセスサーバ１２４において正規のシステム管理者であることが認証されると、アクセスサーバ１２４は、クライアント１３０を、社内ＬＡＮ１２０内のＷＷＷ・ＤＮＳ・メールサーバ１２２に接続する。これによって、クライアント１

３０は、社内ＬＡＮ１２０内のＷＷＷ・ＤＮＳ・メールサーバ１２２にアクセスすることが可能となり、システム管理者の権限によるシステム管理およびファイル管理をおこなうことができる。

【０１０１】

ただし、クライアント１３０とＷＷＷ・ＤＮＳ・メールサーバ１２２と間のデータ送受信においても、データ防護機能付ＴＡ／モデム１３２および１２６を経由するため、これらのシステム管理およびファイル管理をおこなうに際して入力されるコマンドや送受信されるファイルに対しても、実施の形態１において説明した符号化／復号化がおこなわれる。

【０１０２】

すなわち、社内ＬＡＮ１２０に設置されるアクセスサーバ１２４のＴＡ／モデムに、実施の形態１で説明したデータ防護機能が付加されている限り、同データ防護機能が付加されたＴＡ／モデムを備えたクライアントを使用しなければ、社外から社内ＬＡＮのＷＷＷ・ＤＮＳ・メールサーバ１２２にアクセスすることはできない。

【０１０３】

特に、データ防護機能が付加されたＴＡ／モデムを備えたクライアントを使用しなければ、アクセスサーバ１２４が要求するＩＤ番号／パスワード入力をも実行することができないため、ＩＤ番号／パスワード自動生成ツールを使用することによる「なりすまし」の問題も防げることになる。

【０１０４】

ここで、公衆回線１４０としてアナログ回線を使用する場合には、クライアント１３０側およびアクセスサーバ１２４側において、ともにモデムを必要とするが、モデムの場合、デジタルデータからアナログデータに変換するに際して、通常、データ圧縮やフレーム化をおこなっている。

【０１０５】

したがって、モデムにおいては、上記データ防護機能を付加させるタイミングが幾通り存在する。図７は、データ防護機能付きモデムの一例を示すブロック図である。図７において、データ防護機能付きモデムは、従来のモデムにおいて送

信処理部を構成するバッファ１５１、データ圧縮部１５２、フレーム処理部１５３、変調処理部１５４およびＤ／Ａコンバータ１５５と、受信処理部を構成するバッファ１６１、データ解凍部１６２、データ抽出処理部１６３、復調処理部１６４およびＡ／Ｄコンバータ１６５と、に加えて、図１に示したデータ防護処理装置１０を備えている。

【０１０６】

特に、データ防護処理装置１０は、データ送信時に、データ圧縮部１５２によって圧縮されたデジタルデータに対して符号化処理を施し、符号化されたデータをフレーム処理部１５３へと受け渡している。また、逆に、データ受信時には、データ抽出処理部１６３によって抽出されたデジタルデータに対して復号化処理を施し、復号化されたデータをデータ解凍部１６２へと受け渡している。

【０１０７】

これによって、モデムとデータ防護処理装置とを一体化することができるとともに、データ圧縮後のコンパクトなデータに対して符号化をおこなうことから、送信するデジタルコンテンツに対して施す符号化処理を削減することができ、データの機密性をともなった、より高速なデータ送受信が可能となる。

【０１０８】

以上に説明したように、実施の形態２にかかるデータ防護処理装置およびデータ防護処理方法によれば、社外のクライアント１３０側と社内のアクセスサーバ１２４側のそれぞれのモデム／ＴＡに、実施の形態１で説明したデータ防護機能を付加することによって、それら二者間のみにおいて正常な通信が可能になるので、アクセスサーバ１２４が外部との接続を許可する社内のサーバに対しては、データ防護機能を有するクライアントのみがアクセス可能となり、他のクライアントからの不正侵入を防止することができる。

【０１０９】

また、以上に説明した実施の形態２にかかるデータ防護処理装置においては、一種類だけの防護キー値を設定していたが、複数の値から構成されるデータパターンを用意しておき、付加範囲の先頭から順に、そのデータパターンが順次示す値を、加算または減算してもよい。

【０１１０】

また、以上に説明した実施の形態２にかかるデータ防護処理装置において、実施の形態１において説明したのと同様に、付加条件／付加範囲／防護キー記憶部３０に記憶される付加条件、付加範囲および防護キー値は、外部より書き換え可能にすることもできる。

【０１１１】

（実施の形態３）

つぎに、実施の形態３にかかるデータ防護処理装置およびデータ防護処理方法について説明する。実施の形態３は、実施の形態１にかかるデータ防護処理装置およびデータ防護処理方法を、上述したインターネットアクセス方法に適用した例を説明するものである。したがって、実施の形態１において説明した内容については同様であるのでその説明は省略する。

【０１１２】

図８は、実施の形態３にかかるデータ防護処理装置およびデータ防護処理方法の適用例を示すシステム構成図である。図８においては、システム管理者の使用するクライアント２５０が公衆回線２６０、インターネット・サービス・プロバイダ２１０、インターネット１００およびインターネット・サービス・プロバイダ１１０を介して、社内ＬＡＮ２２０のバリア・セグメントに位置するＷＷＷ・ＤＮＳ・メールサーバ２２２にアクセスする場合を示している。

【０１１３】

図８において、社内ＬＡＮ２２０は、専用線を介してインターネット・サービス・プロバイダ１１０に接続されており、インターネット・サービス・プロバイダ１１０は、ルータＲ１０をインターネット１００のバックボーンに接続している。これによって、社外のクライアントは、インターネット１００、インターネット・サービス・プロバイダ１１０のルータＲ１０、社内ＬＡＮ２２０内のルータＲ４０を介して、社内ＬＡＮ２２０内のバリア・セグメントに位置するＷＷＷ・ＤＮＳ・メールサーバ２２２にアクセスすることが可能になっている。

【０１１４】

また、社内ＬＡＮ２２０は、ファイアウオールとしてプロキシサーバ２４０を

備えており、社内のクライアント２３８は、社内向けのＤＮＳ・メールサーバ２３６と社外向けのWWW・ＤＮＳ・メールサーバ２２２との間のデータ送受信、ならびにインターネットとの接続をフィルタリングしている。

【０１１５】

図８において、インターネットアクセス方法に実施の形態１にかかるデータ防護処理装置およびデータ防護処理方法を適用するには、クライアント２５０側と、社内ＬＡＮ２２０内のWWW・ＤＮＳ・メールサーバ２２２側とに、それぞれ実施の形態１において説明したデータ防護処理装置を設ける。

【０１１６】

この際特に、クライアント２５０側では、ＴＡ／モデム２５４とクライアント２５０との間に、WWW・ＤＮＳ・メールサーバ２２２側では、ＬＡＮボード２２６とWWW・ＤＮＳ・メールサーバ２２２との間に、それぞれデータ防護処理装置を配置する必要がある。

【０１１７】

ここで、インターネットではＯＳＩ（Ｏｐｅｎ　Ｓｙｓｔｅｍ　Ｉｎｔｅｒｃｏｎｎｅｃｔｉｏｎ）参照モデルのうち、物理層／データリンク層をＥｔｈｅｒｎｅｔとし、トランスポート層／ネットワーク層をＴＣＰ／ＩＰとした通信プロトコルが主流であり、これら通信プロトコルに基づいて送受信されるデータ単位、すなわちデータフレーム（またはデータパケット）は、各通信プロトコルに準じたデータをカプセル化して生成されている。

【０１１８】

たとえば、最下層となるＥｔｈｅｒｎｅｔフレームは、ＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレス等を含んだＥｔｈｅｒｎｅｔヘッダ部とＥｔｈｅｒｎｅｔデータ部から構成される。そして、Ｅｔｈｅｒｎｅｔデータ部は、ＩＰアドレス等を含んだＩＰヘッダ部とＩＰデータ部とから構成される。また、ＩＰデータ部は、ポート番号等を含んだＴＣＰヘッダ部とＴＣＰデータ部とから構成される。さらに、ＴＣＰデータ部には、アプリケーション層に位置するＨＴＴＰ（Ｈｙｐｅｒｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）やＦＴＰ（Ｆｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）等のヘッダ部とデータ

部から構成される。

【０１１９】

また、ＬＡＮやインターネット接続を実現するために必須となるネットワーク機器は、そのレベルに応じて、通信回線上に伝送されているＥｔｈｅｒｎｅｔフレームから、上記した各通信プロトコルのヘッダ部の内容を読み出している。たとえば、スイッチング・ハブは、Ｅｔｈｅｒｎｅｔヘッダ部からＭＡＣアドレスを抽出して経路制御をおこなっており、ルータは、ＩＰヘッダ部からＩＰアドレスを抽出して経路制御をおこなっている。さらに、プロキシサーバでは、ＴＣＰヘッダ部からポート番号を抽出してフィルタリングをおこなっている。

【０１２０】

このようにインターネット標準プロトコルに基づいて伝送されるデータフレームは、ＨＴＴＰアプリケーション層レベルのＨＴＴＰやＦＴＰのデータ部に対してのみ変容させる自由度があり、その他のデータフレーム構成部分について不用意に符号化をおこなってしまうと、送信先に到達しないおそれが高くなる。

【０１２１】

そこで、実施の形態３にかかるデータ防護処理装置およびデータ防護処理方法では、実施の形態１に示したデータ防護処理装置およびデータ防護処理に加え、上記したデータフレームを構成するデータのうち符号化／復号化をおこなうデータ部分を指定する機能を付加している。

【０１２２】

図９は、実施の形態３にかかるデータ防護処理装置の概略構成を示すブロック図である。なお、図９において、図１と共通する部分については同一符号を付してその説明を省略する。図９に示すデータ防護処理装置２０において、図１と異なる点は、符号化処理部にフレームバッファ４２、データフレーム抽出処理部４４およびデータフレーム置換処理部４６が追加され、復号化処理部にフレームバッファ５２、データフレーム抽出処理部５４およびデータフレーム置換処理部５６が追加されたことである。

【０１２３】

フレームバッファ４２は、送信しようとするデータ、特にアプリケーション層

以下の階層に位置するＴＣＰデータやＩＰデータが含まれた状態のデータフレームを受け取って保持する記憶部である。また、データフレーム抽出処理部４４は、フレームバッファ４２に保持されたデータフレームから、ＨＴＴＰデータ等のアプリケーション層に位置するデータを抽出し、抽出したデータを第１送信バッファ２２に書き込む処理をおこなう。

【０１２４】

そして、データフレーム置換処理部４６は、フレームバッファ４２に保持されたデータフレームのうちデータフレーム抽出処理部４４によって抽出されたデータ部分を、第２送信バッファ２８から読み出したデータ、すなわち実施の形態１に説明した符号化処理が施されたデータに置換する処理をおこなう。

【０１２５】

一方、フレームバッファ５２は、受信したデータ、特にアプリケーション層以下の階層に位置するＴＣＰデータやＩＰデータが含まれた状態のデータフレームを受け取って保持する記憶部である。また、データフレーム抽出処理部５４は、フレームバッファ５２に保持されたデータフレームから、ＨＴＴＰデータ等のアプリケーション層に位置するデータを抽出し、抽出したデータを第１受信バッファ３８に書き込む処理をおこなう。

【０１２６】

そして、データフレーム置換処理部５６は、フレームバッファ５２に保持されたデータフレームのうちデータフレーム抽出処理部５４によって抽出されたデータ部分を、第２受信バッファ３２から読み出したデータ、すなわち実施の形態１に説明した復号化処理が施されたデータに置換する処理をおこなう。

【０１２７】

これによって、クライアントやサーバで生成された通信データのうち、通信機器の制御に影響されないデータ部分のみに対して、実施の形態１に説明した符号化／復号化処理をおこなうことができる。

【０１２８】

つぎに、図８において、システム管理者がクライアント２５０をもちいて社内ＬＡＮ２２０のWWW・ＤＮＳ・メールサーバ２２２のファイル管理をおこなう

場合の動作について説明する。まず、システム管理者は、所定のアプリケーション・プログラムによってデータ防護処理装置２５２の機能を切り離しておく。すなわち、クライアント２５０は、実施の形態１に説明した符号化／復号化処理を実行することなく、ＴＡ／モデム２５４を介した通常の通信をおこなう状態となる。

【０１２９】

この状態で、クライアント２５０は、インターネット・サービス・プロバイダ２１０のアクセスサーバ２１４に対してダイヤルアップ接続をおこなうとともに、アクセスサーバ２１４からユーザ認証を受けることで、インターネット１００との接続を確立する。

【０１３０】

そして、システム管理者は、ＷＷＷブラウザを介して、社内ＬＡＮ２２０のＷＷＷ・ＤＮＳ・メールサーバ２２２のＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を入力する。これによって、クライアント２５０は、ＷＷＷページ送信要求を示した送信データをＴＡ／モデム２５４に送信する。

【０１３１】

ＴＡ／モデム２５４に送信された送信データは、公衆回線２６０を介してインターネット・サービス・プロバイダ２１０のＴＡ／モデム２１６に到達し、アクセスサーバ２１４およびルータＲ３０を介して、インターネット１００のバックボーンへと伝送される。

【０１３２】

インターネット１００のバックボーンへと伝送された送信データは、インターネット・サービス・プロバイダ１１０のルータＲ１０に到達し、社内ＬＡＮ２２０のルータＲ４０へと到達する。ルータＲ４０に到達した送信データは、ＬＡＮボード２２６を介して、ＷＷＷ・ＤＮＳ・メールサーバ２２２に到達する。なお、この際、データ防護処理装置２２４は、ＷＷＷ・ＤＮＳ・メールサーバ２２２によって、その機能が切り離されている。

【０１３３】

そして、ＷＷＷ・ＤＮＳ・メールサーバ２２２は、ＷＷＷサーバ部分が管理す

るホームページを示すデータを、上記した経路と逆の経路を辿ってクライアント２５０に返信する。

【０１３４】

ホームページを示すデータを受け取ったクライアント２５０は、そのホームページをWWWブラウザ上に表示し、この状態で、システム管理用の特別なコマンドを入力する。このコマンドは、上記同様の経路でWWW・ＤＮＳ・メールサーバ２２２に到達する。この際、クライアント２５０は、上記した所定のアプリケーション・プログラムによってデータ防護処理装置２５２の機能を有効にする。また、WWW・ＤＮＳ・メールサーバ２２２においても、上記コマンドを受け取ると、データ防護処理装置２２４の機能を有効にする。

【０１３５】

したがって、これ以降のクライアント２５０とWWW・ＤＮＳ・メールサーバ２２２との通信は、実施の形態１に説明した符号化／復号化処理を経由しておこなわれることになり、他のクライアントを利用している者が、システム管理者をなりすましてWWW・ＤＮＳ・メールサーバ２２２にアクセスすることはできない。

【０１３６】

以上に説明したように、実施の形態３にかかるデータ防護処理装置およびデータ防護処理方法によれば、社外のクライアント２５０側と社内のWWW・ＤＮＳ・メールサーバ２２２側のそれぞれに実施の形態１で説明したデータ防護処理装置を付加してそれらデータ防護処理装置を発動させることによって、二者間のみにおいて正常な通信が可能になるので、WWW・ＤＮＳ・メールサーバ２２２に対しては、データ防護処理装置を有するクライアントのみがアクセス可能となり、他のクライアントからの不正侵入を防止することができる。

【０１３７】

なお、以上の実施の形態３においては、社外から社内ＬＡＮ２２０にアクセスする場合を示したが、社内ＬＡＮ２２０からWWW・ＤＮＳ・メールサーバ２２２にアクセスする場合においても、図８に示すように、システム管理者が使用するクライアント２３０と、ＬＡＮボード２３４との間にデータ防護処理装置２３

２を配置することで、上記同様の作用および効果を享受することができる。

【０１３８】

また、以上に説明した実施の形態２，３にかかるデータ防護処理装置においては、実施の形態１において説明したのと同様に、一種類だけの防護キー値を設定していたが、複数の値から構成されるデータパターンを用意しておき、付加範囲の先頭から順に、そのデータパターンが順次示す値を、加算または減算してもよい。

【０１３９】

また、以上に説明した実施の形態３にかかるデータ防護処理装置においては、実施の形態１において説明したのと同様に、付加条件／付加範囲／防護キー記憶部３０に記憶される付加条件、付加範囲および防護キー値は、外部より書き換え可能にすることもできる。

【０１４０】

また、以上に説明した実施の形態１～３にかかるデータ防護処理方法は、ハードディスクやＣＤ－Ｒドライブ等の記憶媒体にコンピュータプログラムとして記録することにより提供してもよく、その場合は、上述したデータ防護処理装置に代わって、そのコンピュータプログラムが符号化／復号化処理を実行する。

【０１４１】

【発明の効果】

以上説明したように、この発明にかかるデータ防護処理装置によれば、受け取ったデジタルデータが所定の数値であるか否かを判定し、所定の数値であると判定された場合には、その判定後に所定の回数のデジタルデータを受け取った際のそのデジタルデータに対して所定の演算値を加算または減算することによって符号化／復号化を実現するので、送受信する一連のデジタルコンテンツのデジタルデータのすべてを受け取らずとも、実際に受け取った部分から順に符号化／復号化を実行することが可能になり、送信／受信バッファとして大容量のものを必要とすることなく、装置構成を安価にすることができる。また、このデータ防護処理装置を互いに有する二者間においては、データの機密化と高速な送受信をともに実現することができる。

【図面の簡単な説明】

【図１】

実施の形態１にかかるデータ防護処理装置の概略構成を示すブロック図である。

【図２】

実施の形態１にかかるデータ防護処理装置の符号化処理を示すフローチャートである。

【図３】

実施の形態１にかかるデータ防護処理装置において、防護キー値の加算処理を説明するための説明図である。

【図４】

符号化処理によって得られるバイトデータ列の例を示す図である。

【図５】

実施の形態１にかかるデータ防護処理装置の復号化処理を示すフローチャートである。

【図６】

実施の形態２にかかるデータ防護処理装置およびデータ防護処理方法の適用例を示すシステム構成図である。

【図７】

実施の形態２にかかるデータ防護処理装置およびデータ防護処理方法において、データ防護機能付きモデムの一例を示すブロック図である。

【図８】

実施の形態３にかかるデータ防護処理装置およびデータ防護処理方法の適用例を示すシステム構成図である。

【図９】

実施の形態３にかかるデータ防護処理装置の概略構成を示すブロック図である。

【符号の説明】

１０，２０，２２４，２３２，２５２　データ防護処理装置

２２　第１送信バッファ

２４　防護キー付加位置判定部

２６　防護キー付加処理部

２８　第２送信バッファ

３０　付加条件／付加範囲／防護キー記憶部

３２　第２受信バッファ

３４　防護キー除去処理部

３６　防護キー除去位置判定部

３８　第１受信バッファ

４２，５２　フレームバッファ

４４，５４　データフレーム抽出処理部

４６，５６　データフレーム置換処理部

１００　インターネット

１１０，２１０　インターネット・サービス・プロバイダ

１２０，２２０　社内ＬＡＮ

１２２，２２２　ＷＷＷ・ＤＮＳ・メールサーバ

１２４，２１４　アクセスサーバ

１２６，１３２　データ防護機能付ＴＡ／モデム

１２８，１３０，２３０，２３８，２５０　クライアント

１４０，２６０　公衆回線

１５１　バッファ

１５２　データ圧縮部

１５３　フレーム処理部

１５４　変調処理部

１５５　Ｄ／Ａコンバータ

１６１　バッファ

１６２　データ解凍部

１６３　データ抽出処理部

１６４　復調処理部

１６５　Ａ／Ｄコンバータ

２１２，２２２　ＷＷＷ・ＤＮＳ・メールサーバ

２１６，２５４　ＴＡ／モデム

２２６，２３４　ＬＡＮボード

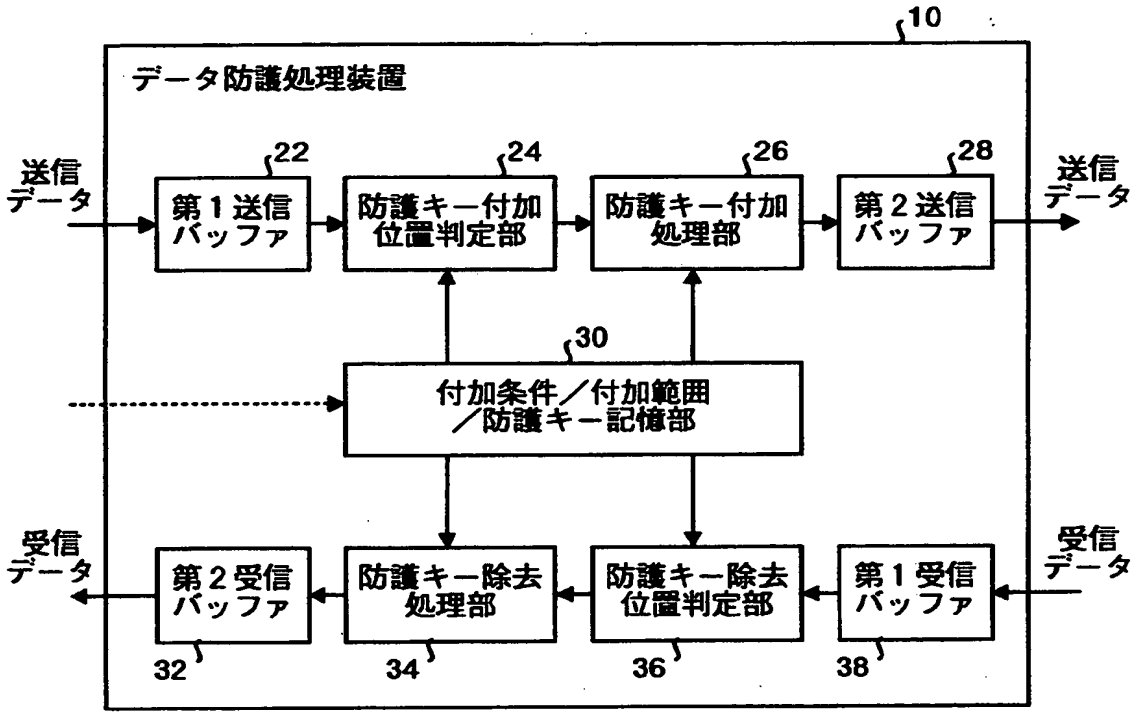
２３６　ＤＮＳ・メールサーバ

２４０　プロキシサーバ

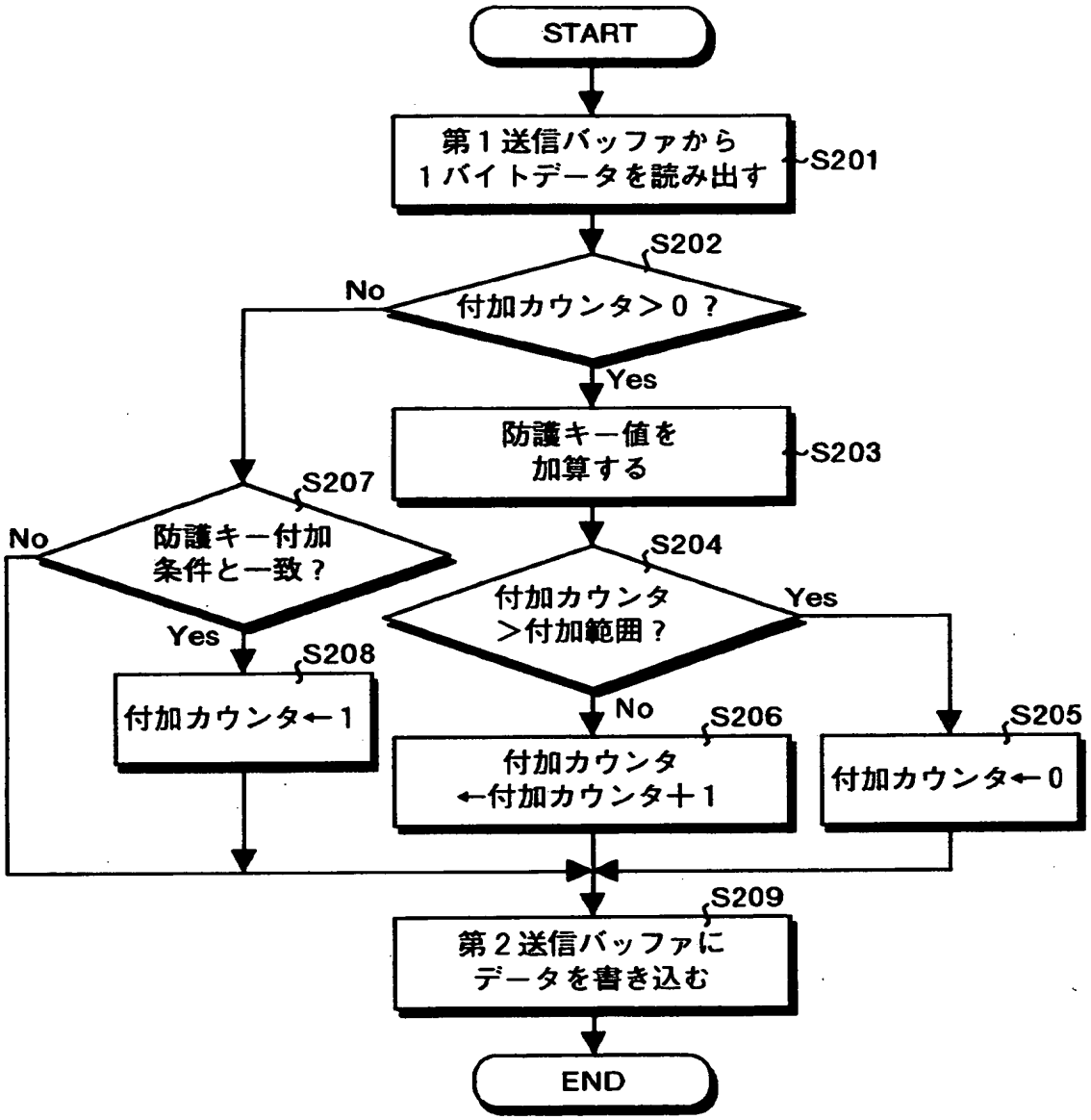
Ｒ１０，Ｒ２０，Ｒ３０，Ｒ４０　ルータ

【書類名】　　図面

【図１】


10
データ防護処理装置
送信データ
22
第１送信バッファ
24
防護キー付加位置判定部
26
防護キー付加処理部
28
第２送信バッファ
送信データ
30
付加条件／付加範囲／防護キー記憶部
受信データ
第２受信バッファ
防護キー除去処理部
防護キー除去位置判定部
第１受信バッファ
受信データ
32
34
36
38

【図２】


START
第１送信バッファから
１バイトデータを読み出す
S201
S202
No
付加カウンタ＞０？
Yes
防護キー値を
加算する
S203
S207
No
防護キー付加
条件と一致？
S204
付加カウンタ
＞付加範囲？
Yes
Yes
S208
付加カウンタ←１
No
S206
付加カウンタ
←付加カウンタ＋１
S205
付加カウンタ←０
S209
第２送信バッファに
データを書き込む
END

【図３】

「防護キー値＝“1E”の場合」

	付加処理前		付加処理後
バイナリコード：	“１０１１００１０”	⇨	“１１０１０００”
	‖		‖
ヘキサコード　：	“B2”		“D0”

【図４】

付加条件　：“5D”のつぎから
防護キー値：“1E”
付加範囲　：３バイト

第１送信バッファ

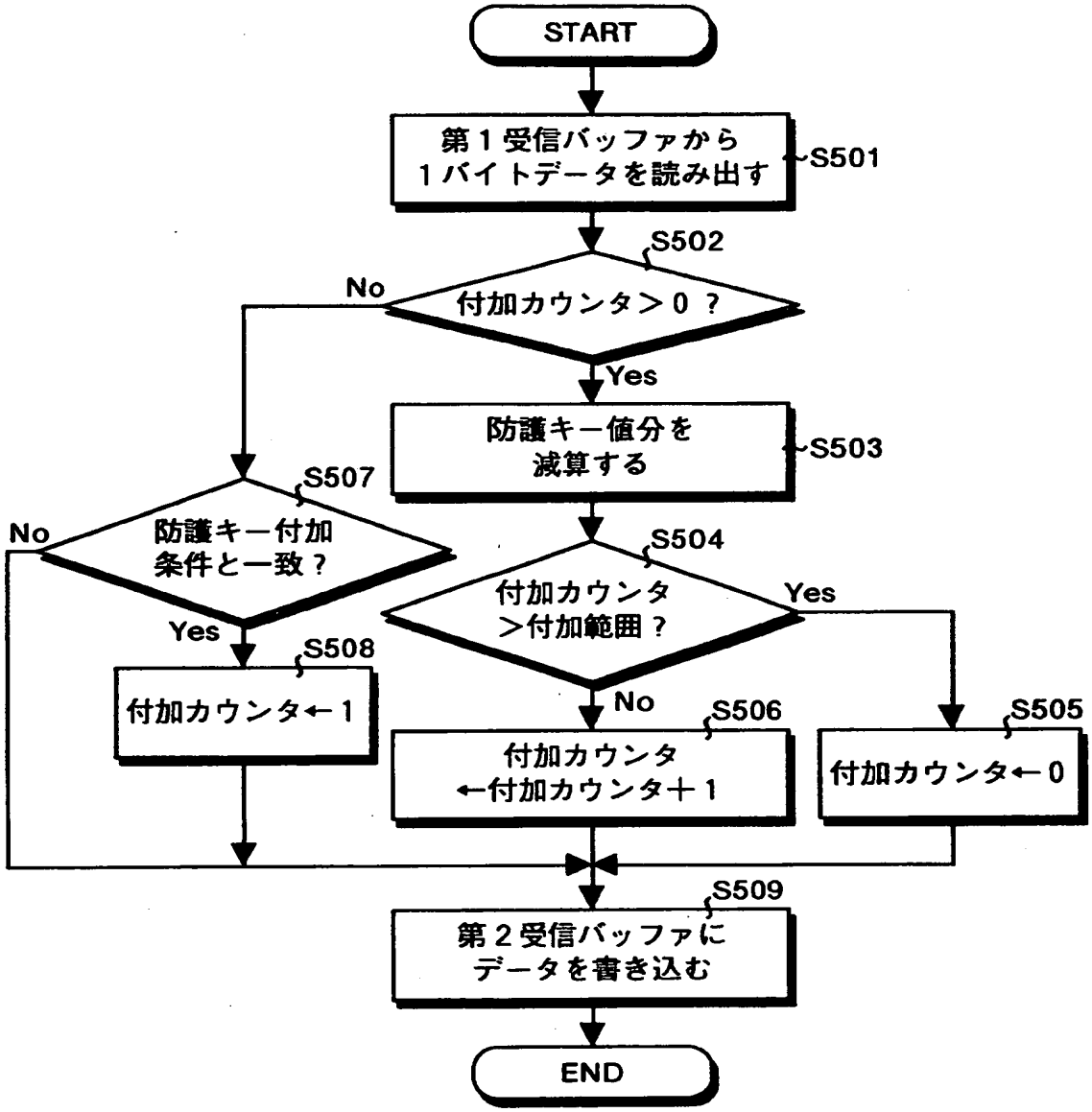
2A 19 6D 3F 5D 9B 11 40 A9 DD E7 38 65 21
5D 88 FA 1B 33 20 DC 56 7A BC 6D 2F ……

⇩

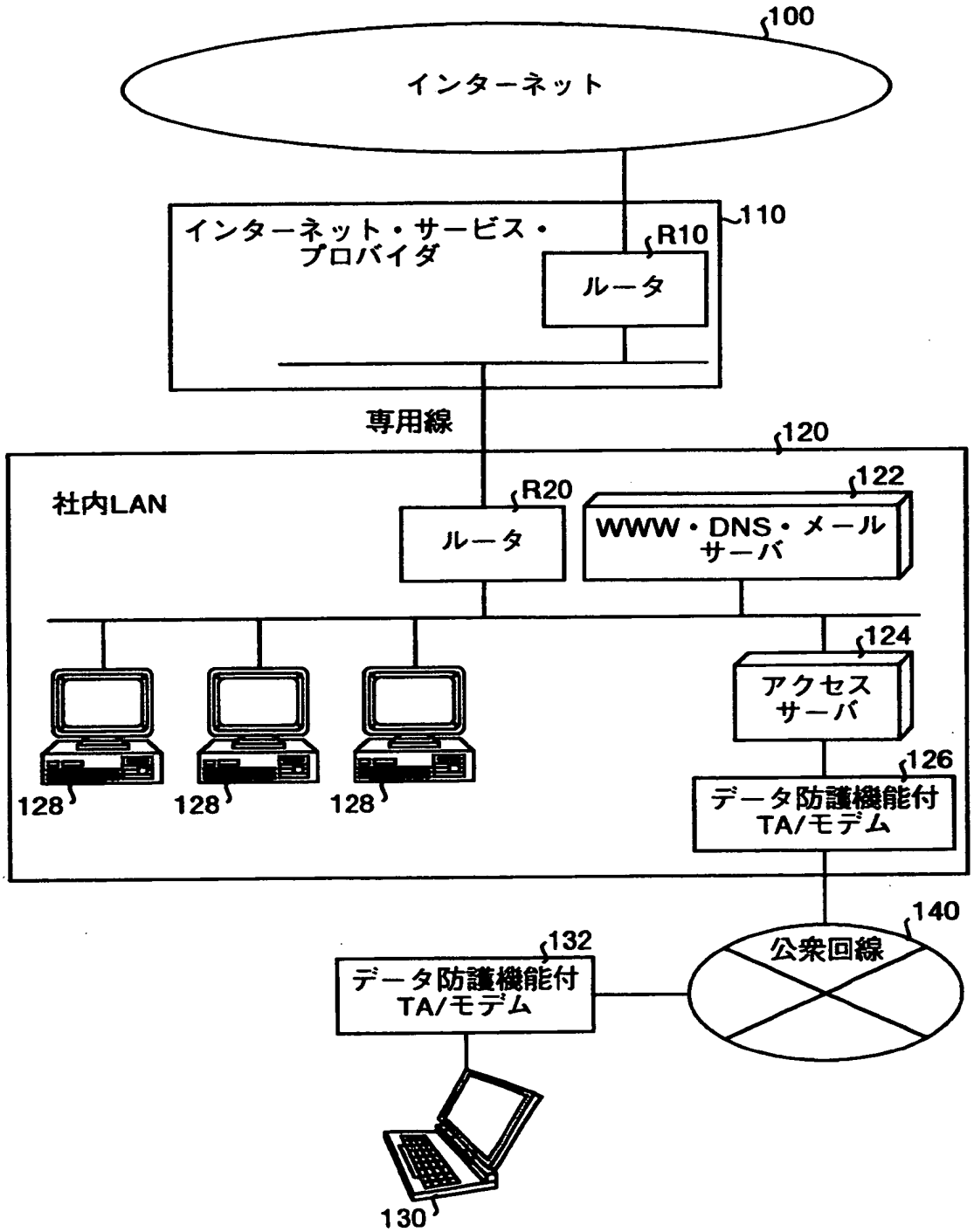
第２送信バッファ

2A 19 6D 3F 5D B9 2F 5E A9 DD E7 38 65 21
5D A6 19 39 33 20 DC 56 7A BC 6D 2F ……

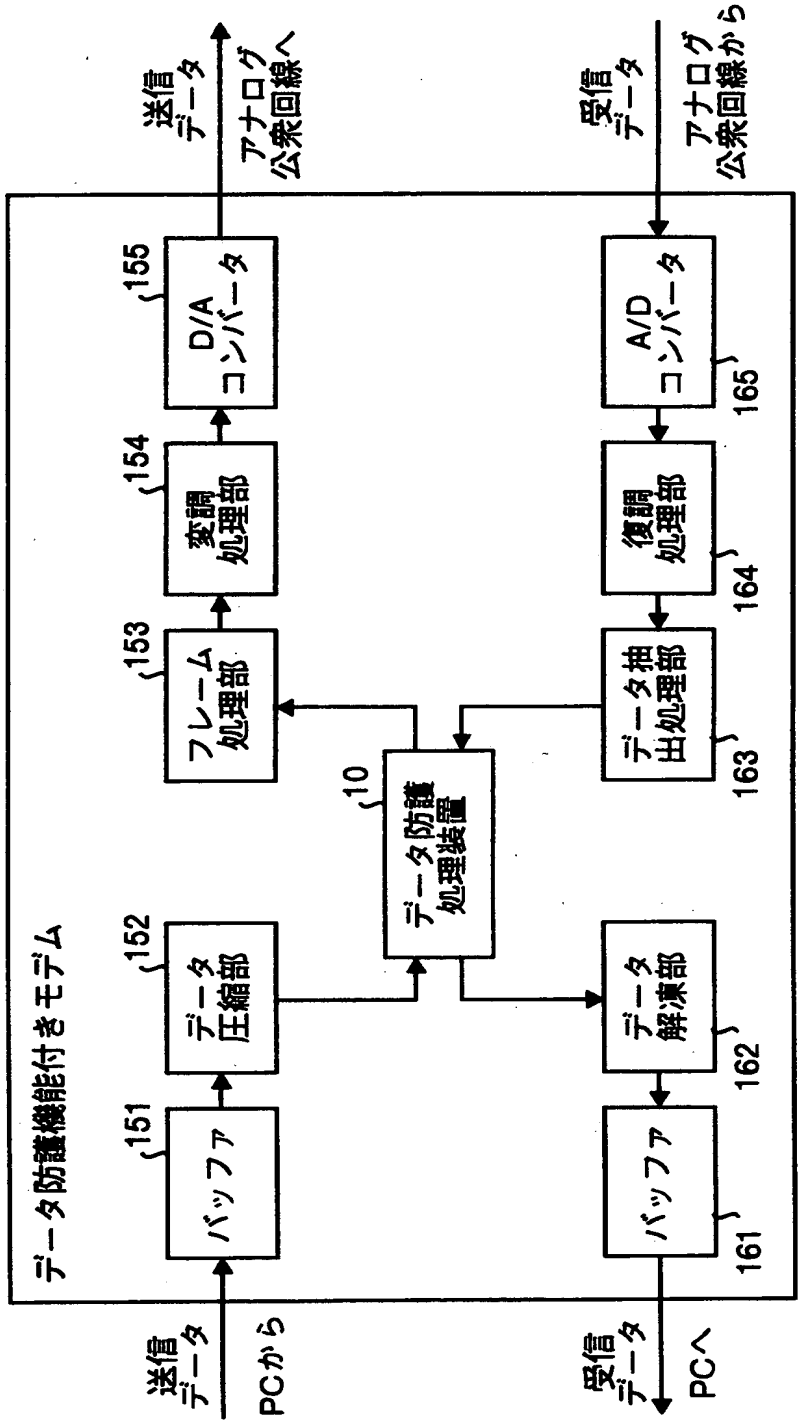
【図５】


START
第１受信バッファから
１バイトデータを読み出す
S501
S502
No
付加カウンタ＞０？
Yes
防護キー値分を
減算する
S503
S507
No
防護キー付加
条件と一致？
S504
付加カウンタ
＞付加範囲？
Yes
Yes
S508
付加カウンタ←１
No
S506
付加カウンタ
←付加カウンタ＋１
S505
付加カウンタ←０
S509
第２受信バッファに
データを書き込む
END

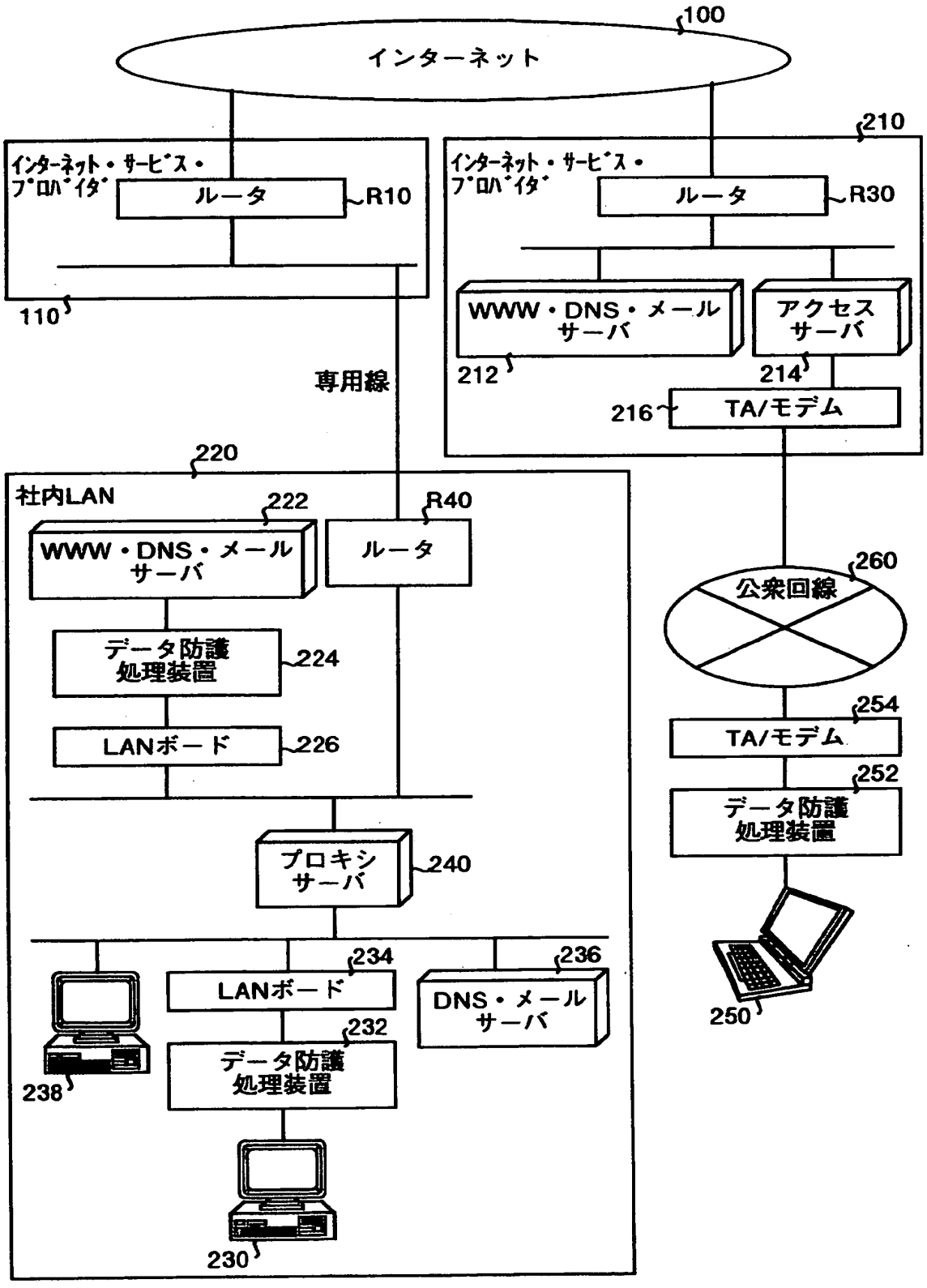
【図６】


100
インターネット
インターネット・サービス・
プロバイダ
110
R10
ルータ
専用線
120
社内LAN
R20
ルータ
122
WWW・DNS・メール
サーバ
124
アクセス
サーバ
126
データ防護機能付
TA/モデム
128
128
128
140
公衆回線
132
データ防護機能付
TA/モデム
130

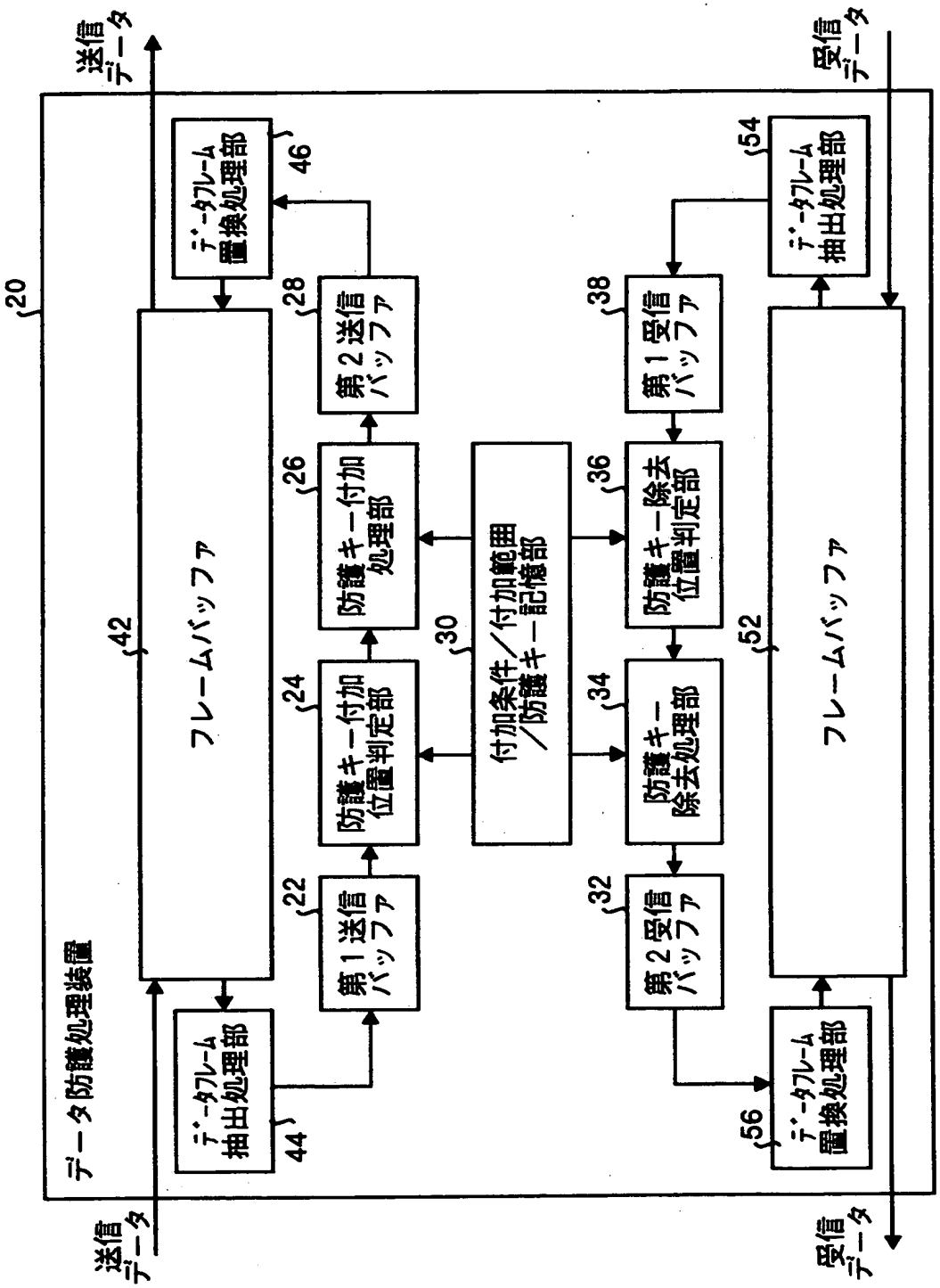
【図７】


データ防護機能付きモデム
送信データ
PCから
受信データ
PCへ
送信データ
アナログ公衆回線へ
受信データ
アナログ公衆回線から
151
バッファ
152
データ圧縮部
153
フレーム処理部
154
変調処理部
155
D/Aコンバータ
161
バッファ
162
データ解凍部
163
データ抽出処理部
164
復調処理部
165
A/Dコンバータ
10
データ防護処理装置

【図８】


100
インターネット
210
ｲﾝﾀｰﾈｯﾄ・ｻｰﾋﾞｽ・ﾌﾟﾛﾊﾞｲﾀﾞ
ルータ
R10
110
ｲﾝﾀｰﾈｯﾄ・ｻｰﾋﾞｽ・ﾌﾟﾛﾊﾞｲﾀﾞ
ルータ
R30
WWW・DNS・メール サーバ
212
アクセス サーバ
214
216
TA/モデム
専用線
220
社内LAN
222
WWW・DNS・メール サーバ
R40
ルータ
260
公衆回線
データ防護 処理装置
224
LANボード
226
254
TA/モデム
252
データ防護 処理装置
プロキシ サーバ
240
234
LANボード
236
DNS・メール サーバ
232
データ防護 処理装置
238
250
230

【図９】


送信データ
受信データ
データ防護処理装置
20
フレームバッファ
42
データフレーム置換処理部
46
第２送信バッファ
28
防護キー付加処理部
26
防護キー付加位置判定部
24
第１送信バッファ
22
データフレーム抽出処理部
44
付加条件／付加範囲／防護キー記憶部
30
第１受信バッファ
38
防護キー除去位置判定部
36
防護キー除去処理部
34
第２受信バッファ
32
データフレーム抽出処理部
54
フレームバッファ
52
データフレーム置換処理部
56
送信データ
受信データ

【書類名】　　要約書

【要約】

【課題】　送受信データをそのデータ・サイズを増大させることなくかつ十分な保安性を高めて符号化／復号化するデータ防護処理装置を提供すること。

【解決手段】　防護キー付加位置判定部２４または防護キー除去位置判定部３６において、受け取ったデジタルデータが所定の付加条件を満たすか否かを判定し、所定の付加条件を満たす場合には、防護キー付加処理部２６または防護キー除去処理部３４において、その判定後に所定の回数のデジタルデータを受け取った際のそのデジタルデータに対して所定の防護キー値を加算または減算することによって符号化／復号化を実現する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔３０００２３３８３〕

１．変更年月日　　２０００年　３月１６日
［変更理由］　新規登録
住　所　徳島県徳島市川内町平石住吉２０９番地５
氏　名　株式会社トリニティーコミュニケーション